TIETOTURVASUUNNITELMA SEKÄ TIETOVERKON JA VARMUUSKOPIOINTIRATKAISUN SUUNNITTELU AV-TIIMI LJ OY:LLE

Jouni Ikonen

Opinnäytetyö

Ammattikorkeakoulututkinto

Savonia ammattikorkeakoulu

SAVONIA-AMMATTIKORKEAKOULU **OPINNÄYTETYÖ**
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Jouni Ikonen	
Työn nimi Tietoturvasuunnitelma sekä tietoverkon ja varmuuskopiointiratkaisun suunnittelu AV-Tiimi LJ Oy:lle	
Päiväys 6.5.2011	Sivumäärä/Liitteet 55
Ohjaaja(t) Tietohallintopäällikkö, Matti Kuosmanen. Toimitusjohtaja, Leena Jälkö.	
Toimeksiantaja/Yhteistyökumppani(t) AV-TIIMI LJ Oy	

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli laatia Keravalla toimivalle AV-alaan erikoistuneelle yritykselle tietoturvasuunnitelma. Työhön sisällytettiin myös tietoverkkopohjaisen tiedonvarmennusratkaisun suunnittelu ja nykyisen tietoverkon uudistamisen kartoittaminen. Yrityksen tiedon suojaaminen on tärkeää toiminnan jatkumisen kannalta.

Ensin toimitusjohtajan kanssa kartoitettiin yrityksen nykyisen tietoturvan taso. Puutteet ja toiveet kirjattiin, jotta niihin voitiin paneutua työn myöhemmissä vaiheissa. Työssä käsiteltiin myös tietoturvaan liittyviä käsitteitä sekä erilaisia varmuuskopiointiratkaisuja. Tarkemmin tutustuttiin NAS-tyyppiseen tiedonvarmennusratkaisuun. Tietoverkon ja varmuuskopiointiratkaisun suunnittelussa otettiin huomioon myös liiketoiminnan mahdollinen laajentuminen tulevaisuudessa. Teoriatietoa aiheesta haettiin alan kirjallisuudesta sekä internetjulkaisuista. Työn käytännön toteutus siirtyi yrityksen toiveesta tuonnemmaksi.

Työssä toteutettiin tietoturvasuunnitelma AV-Tiimille, jossa esiteteltiin huomatut puutteet yrityksen teknisessä sekä fyysisessä tietoturvassa sekä ratkaisut niihin. Lopuksi työssä esitettiin tarvittavat ratkaisut ja hankinnat tietoverkon uudistamista varten.

Avainsanat
Tietoturva, NAS, palomuuri, tietoverkko

Julkinen

SAVONIA UNIVERSITY OF APPLIED SCIENCES **THESIS**
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Computer Science			
Author(s) Jouni Ikonen			
Title of Thesis Information Security Plan and Network Design and Backup Solution for AV-Tiimi LJ Ltd			
Date	6 May 2011	Pages/Appendices	55
Supervisor(s) Mr Matti Kuosmanen, Information System Manager Ms Leena Jälkö, CEO			
Project/Partners AV-TIIMI LJ Ltd.			

Abstract

The purpose of this thesis was to draw up an information security plan for a company which specializes in audio and visual business. Another purpose was to improve their current network topology. Securing information is very valuable and important when planning the continuity of the company's operations.

The thesis was started by a meeting with the company's CEO to map out the possible gaps in AV-Tiimi's current information security. Inadequacies and requests were written down so that they could be met in the later stage. Facts concerning working information security were also studied. Various backup methods were also studied, the emphasis being on a NAS type solution. Theoretical information was searched from world wide web and also from literature.

As a result of this thesis an information security plan for AV-Tiimi LJ Ltd was implemented. It outlines the deficiencies noted earlier in the process and suggests solutions for them. It also describes the solution for the enterprise's data backup. Finally, the thesis provides the necessary solutions for the renovation of the current intranet.

Keywords
Information security, NAS, firewall, network

Public

SISÄLTÖ

LYHENTEET

AES Advanced Encryption Standard

CD Compact Disc

CIFS Common Internet Filesystem

DAS Direct Attached Storage

DHCP Dynamic Host Configuration Protocol

DVD Digital Versatile Disc tai Digital Video Disc

DMZ Demilitarized Zone

GRE Generic Routing Encapsulation

IANA Internet Assigned Numbers Authority

ICT Information and Communications Technology, suom. Tieto ja viestintäteknologia

IDS Intrusion Detection System

IEEE Institute of Electrical and Electronics Engineering

IEC Internation Electrotechnical Commission

IP Internet Protocol

IPSec Internet Protocol Security

ISO Internal Organization for Standardization

LAN Local Area Network

NFS Network File System

MAC Media Access Control

NAS Network-Attached Storage tai Network Access Storage

NAT Network Address Translation

PC Personal Computer

PIN Personal Identification Number

PPTP Point-to-Point Tunneling Protocol

RAID Reduntant Array of Independent Disks

RAM Random Access Memory

USB	Universal Serial Bus
UPS	Uninterruptible Power Supply
SAN	Storage Area Network
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier
SSL	Secure Sockets Layer
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

1 JOHDANTO

Tietotekniikan tarkoituksena on helpottaa käyttäjiensä arjen toimintoja, mitä se oikein toimiessaan tekeekin. Toimimaton tietotekniikka voi toisaalta huonontaa yrityksen tulosta ja altistaa yrityksen monenlaisille riskeille. Esimerkiksi yrityksen huonosti konfiguroitu palomuuri voi avata tien hakkerille hyvinkin salaisiin tietoihin. Vahingossa väärään osoitteeseen lähetetty tarjoussähköposti paljastaa luottamuksellisia hintatietoja toiselle asiakkaalle tai pahimmassa tapauksessa jopa kilpailevalle yritykselle.

Turvallisuus onkin juuri toimintojen jatkuvuuden suunnittelua ongelmien sattuessa sekä riskien minimoimista. Tietoturvallisuudella pyritään minimoimaan riskejä arkaluontoisen tiedon väärinkäyttöön ja turvaamaan tietoteknisiä laitteita. Riskejä voidaan joko tutkia tai ehkäistä ennalta. Tutkivat menetelmät etsivät ja tunnistavat riskejä ennen vahingon tapahtumista, ja ennaltaehkäisevät pyrkivät estämään ei-haluttuja tapahtumasta.

Riskeistä huolimatta yritykset eivät täysin tiedosta tietoturvan merkitystä. Tietoturvan suunnittelu vaatiikin suurta panosta yrityksen johdolta, jotta päästään tehokkaaseen tulokseen. Tehokasta tulosta ei myöskään saavuteta ellei suunnitteluun oteta mukaan kaikkia henkilöitä, joita suunnitelma koskee.

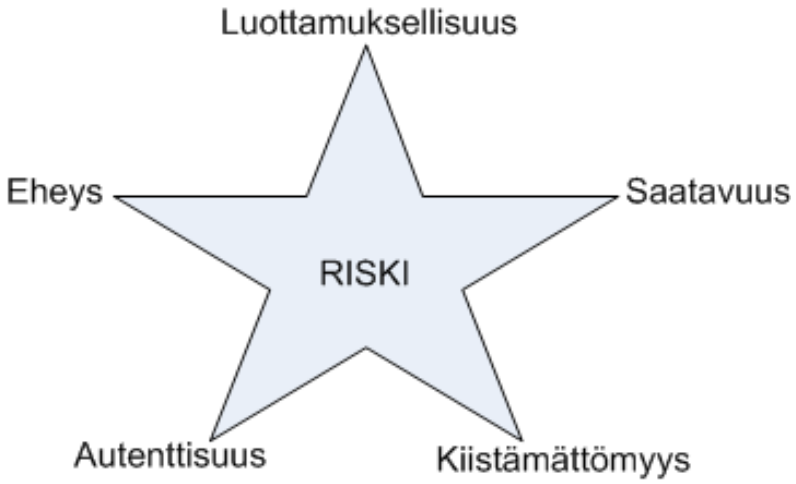
Työ tehdään AV-Tiimi LJ Oy:lle. Ajatus työn aiheesta syntyi yrityksen miettiessä parempaa tapaa hoitaa tietojensa varmuuskopiointi. Opinnäytteen tarkoituksena on laatia tietoturvasuunnitelma, suunnitella verkkopohjainen tiedonvarmennusratkaisu sekä uudistaa pienyrityksen tietoverkko.

2 YLEISTÄ TIETOTURVASTA

Kuten johdannossa jo todettiin, tietoturvan tarkoituksena on ehkäistä riskejä ja varmistaa, että kaikki tietotekniset laitteet ja ohjelmistot toimivat kuten niiden pitääkin.

2.1 CIA-malli ja turvallisuustähti

Suurimmassa osassa alan julkaisuja sekä monessa kansainvälisessä yrityksessä tietoturvan tavoitteet jaetaan ns. CIA-mallin mukaisesti. CIA-lyhenne tulee sanoista confidentiality, integrity sekä availability, jotka suomennettuna tarkoittavat luottamuksellisuutta, eheyttä sekä saatavuutta. Tämä malli on laajennettu myös niin kutsutuksi turvallisuustähdeksi. CIA-malliin lisätään kaksi uutta tavoitetta, autenttisuus sekä kiistämättömyys. (Raggad 2010, 22.)



KUVA 1. Turvallisuustähti (Raggad 2010, 22).

Luottamuksellisuuden tavoite on varmistaa, että tietojärjestelmän tietoja pystyvät käyttämään vain siihen oikeutetut käyttäjät (Ruohonen 2002, 2). Esimerkiksi asiakastietoja sisältävien dokumenttien huolimaton jakelu voi johtaa tietojärjestelmän luottamuksellisuuden menetykseen.

Saatavuuden tavoite on, että tietojärjestelmän tiedot ovat aina käyttäjien käytettävissä. Käyttäjän näkökulmasta tämä on tietojärjestelmän tärkein ja näkyvin palvelu, ja tietojärjestelmän ylläpitäjän näkökulmasta tämä on vaikeimmin saavutettava ja monimutkaisin palvelu (Ruohonen 2002, 3).

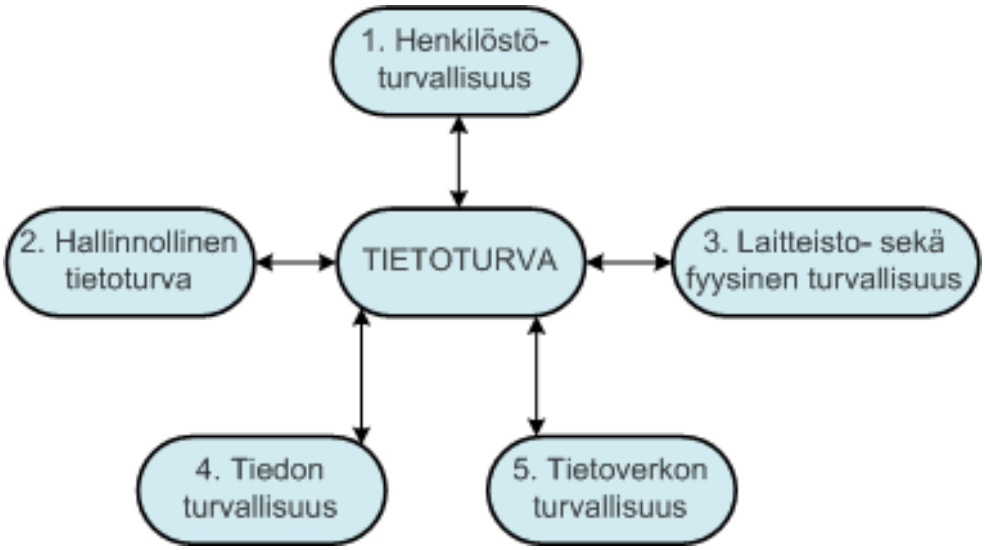
Eheyden tavoite on, että tietojärjestelmän tiedot eivät pääse muuttumaan – vahingossa tai tarkoituksella – ilman, että käyttäjä, joka on oikeutettu niiden muuttamiseen tekee muutoksen (Ruohonen 2002, 3). Esimerkiksi virus tai mato, joka korruptoi tietoja voi johtaa tietojärjestelmän eheyden menetykseen.

Autenttisuuden tavoitteena on, että kaikki tietojärjestelmän osat voidaan tunnistaa luotettavasti (Ruohonen 2002, 2). Useimmiten pääsy järjestelmään vaatii jotain mitä käyttäjä tietää. Esimerkiksi salasanan ja käyttäjätunnuksen. Muita tapoja käyttäjän tunnistamiseen on monia kuten biometriikka sekä älykortit. Erilaisten tunnistamistapojen yhdistely kasvattaa tietojärjestelmän tietoturvaa.

Kiistämättömyyden tavoite on, että kaikki tietojärjestelmässä tapahtuneet tapahtumat voidaan myöhemmin todentaa luotettavasti (Ruohonen 2002, 3). Kiistämättömyyden saavuttamiseksi voidaan käyttää esimerkiksi dokumenttien digitaalista allekirjoitusta.

2.2 Tietoturvan osa-alueet

Tietoturva voidaan jakaa eri osa-alueisiin. Alla olevassa kuvassa tietoturva jaetaan viiteen eri osa-alueeseen.



KUVA 2. Tietoturvan osa-alueet.

Henkilöstöturvallisuus tarkoittaa yrityksen tietojärjestelmän suojaamista sitä käyttäviltä henkilöiltä. Tämä tarkoittaa käyttäjien käyttöoikeuksien rajoittamista, palkattavien henkilöiden taustojen tarkastamista sekä käytön opastusta.

Hallinnollinen tietoturva tarkoittaa tietoturvan johtamista. Yrityksen hallinto sitoutuu luomaan tietoturvan kehitystä ohjaavan tietoturvasuunnitelman sekä noudattamaan siinä ehdotettuja ratkaisuja.

Laitteisto- ja fyysinen turvallisuus sisältää tietojärjestelmän laitteiden suojaamisen, oli laite sitten kannettava tietokone tai vaikkapa yrityksen runkoverkon reititin.

Fyysinen turvallisuus tarkoittaa itse yrityksen tilojen turvaamista esimerkiksi erilaisin kulunvalvontajärjestelmin, palovaroittimin ja vartiointipalveluin. Fyysisen turvallisuuden ei aina ajatella kuuluvan tietoturvaan, mutta käytännössä sillä on suuri merkitys tietoturvalle (Ruohonen 2002, 4 - 5).

Tiedon tietoturva jaottelee yrityksen tiedon erilaisiin osiin, joiden perusteella yrityksessä olevaa tietoa tulisi suojata. On olemassa ns. julkista tietoa, erittäin salaista tietoa sekä erilaisia luokituksia näiden kahden väliltä. Julkisena tietona voidaan pitää esimerkiksi yrityksien vuosikertomuksia, tilinpäätöksiä ja www-sivuja. Eli kaikkea tietoa, joka on yleisesti ja laillisesti saatavilla olevaa. Erittäin salaista tietoa voivat esimerkiksi olla osa asevoimien dokumentteja ja yrityksen tuotekehittelyprosessista syntyneitä dokumentaatioita. Yleisesti erittäin salaista tietoa sisältävät kohteet ovat eristettyjä muusta tietoverkosta ja niiden käyttö vaatii vahvaa tunnistautumista.

ISO ja IEC ovat julkistaneet ISO/IEC 27002-standardin, jossa tieto luokitellaan viiteen eri osa-alueeseen: julkiseen, sisäiseen, omaan, luottamukselliseen ja erittäin salaiseen (Raggad 2010, 7).

Tietoverkon turvallisuus käsittää tietojärjestelmän ulkopuolisen tietoliikenteen turvaamista. Tietoverkkojen turvallisuutta voidaan kasvattaa käyttämällä palomuureja, salakirjoittamista sekä esimerkiksi etätyöntekijöillä VPN-yhteyksiä.

3 TIETOTURVARISKIT JA NIIHIN VARAUTUMINEN

Tietojärjestelmissä on monenlaisia riskejä. Palvelinhuoneen jäähdytysjärjestelmän rikkoontuminen, pääjohtajan kiintolevyn hajoaminen, valvomattomasta varaston ovesta sisään kävellyt varas tai vaikkapa selaimen tietoturva-aukkoa hyväksikäyttänyt hakkeri voivat saada aikaan suuriakin menetyksiä ja kuten esimerkeistä huomataan tietoturvariskit ovatkin välillä aivan jotain muuta, kuin perinteisiksi luullut sähköpostin liitetiedostona tai varomattoman internetselailun sivutuotteena saadut madot ja troijalaiset.
Kaikkiin edellämainuttuihin voidaan, ja niihin tulisikin varautua ennalta. Tuuletusjärjestelmien ja kiintolevyjen ollessa mekaanisia laitteita voidaan niiden olettaakin vikaantuvan jossakin vaiheessa niiden käyttöikää, sillä eihän mikään mekaaninen laite loputtomiin käyttöä kestä. Toimiva tietoturva koostuu enemmänkin pienistä, kuin suurista asioista. Toimiva varmuuskopiointijärjestelmä, ajan tasalla oleva antivirusohjelmisto, oikein säädetty palomuuri, hyvä salasanapolitiikka, kriittisten järjestelmien vikasietoisuuden varmistaminen ja terve järki vievät jo pitkälle.

Mutta edelleen usein näkee tapauksia, jolloin tilanteeseen reagoidaan vasta silloin, kun vahinko on jo tapahtunut.

Helpoiten yritys voi varautua uhkiin laatimalla tietoturvasuunnitelman. Tietoturvasuunnitelman laatimisen tavoite on varmistaa, että jokainen tietojärjestelmän osa suojataan riittävän tehokkaasti siihen kohdistuviin riskeihin verrattuna. Näin voidaan varmistaa, että tietojärjestelmä on riittävän turvallinen ja ettei tietoturva kuluta ylimääräisiä resursseja (Ruohonen 2002, 6).

Ensimmäinen vaihe tietoturvasuunnitelman laatimisessa on riskien ja tietojärjestelmän osille halutun tietoturvatason määrittäminen. Tavoitteita asettaessa tulisi kuitenkin käyttää maalaisjärkeä ja ymmärtää, että liian utopististen tavoitteiden asettaminen ei hyödytä yritystä eikä yrityksen tietoturvasta vastaavaa työntekijää. Riskejä määrittäessä voidaan käyttää riskianalyysiä ja riskit voidaan jaoetella esimerkiksi sisäisiin, ulkoisiin, tahattomiin ja ennalta arvaamattomiin uhkiin. Tietoturvasuunnitelmaan tulisi myös listata ne toimenpiteet joilla valitut tavoitteet saavutetaan. Näitä toimenpiteitä voidaan kuvata esimerkiksi käytännön ohjein, jotka sisältävät ohjeita oikeanlaisesta salasanapolitiikasta, ohjelmien käytöstä tai kuinka toimia poikkeustilanteessa.

Tekniset dokumentit taas pitävät sisällään tietoa järjestelmän ylläpitäjille. Ne voivat sisältää salasanoja, IP-osoitteita, topologiakuvauksen yrityksen verkosta ja niin

edelleen. Suunnitelmaan tulisi lisätä myös kenen vastuulla tietyn palvelun, esimerkiksi sähköpostipalvelimen tai koko tietoverkon, tietoturva on. Näin selkiytetään pääkäyttäjien tehtäväkenttää. Tietoturvasuunnitelmaan mahdollisesti liitettävä toipumissuunnitelma kuvaa mitä tapahtuu mahdollisen tietomurron tai murron yrityksen jälkeen, jotta tietojärjestelmä saatetaan samanlaiseen toimintakuntoon, jossa se oli ennen tietomurtoa. Kuten myös kaikkea muuta tietoturvaan liittyvää, myös tietoturvasuunnitelmaa tulisi päivittää vastaamaan yrityksessä tapahtuvia muutoksia, jotta tietoturvan taso vastaisi järjestelmän riskejä.

4 HENKILÖSTÖTURVALLISUUS

Henkilöstöturvallisuudella tarkoitetaan henkilöstöstä aiheutuvien riskien hallintaa. Tietoturvallisuuden alaterminä henkilöstöturvallisuudella tarkoitetaan henkilöstöönliittyvien salassapito- ja käytettävyysriskien hallintaa tietoja ja tietojärjestelmiä käytettäessä. Henkilöstöturvallisuustyö on luonteeltaan ennalta ehkäisevää (Valtiovarainministeriö 2008, 11-12).

Henkilöstöturvallisuus onkin yksi tietoturvan tärkeimpiä osa-alueita sillä kaikki yrityksen tieto kulkee henkilöstön kautta. Tiedon ollessa immateriaalista voi epärehellinen työntekijä helposti vaikkapa kopioida yrityksen tietoa ja jakaa sitä edelleen yrityksen ulkopuolella, tai vaikkapa yrityksen tietoa katoaa puhtaasti vahingossa.

Henkilöstöturvallisuuteen vaikuttaa suuresti yrityksessä käytetty henkilöstöpolitiikka, sillä työpaikkaansa tyytyväiset työntekijät työskentelevät yrityksessä pidempään ja ovat myös muutenkin sitoutuneet työpaikkaansa, tyytymättömiä henkilöitä, paremmin.

Yrityksen tulisi määrittää henkilöstölle heidän työnsä toimenkuva, mahdolliset sijaisjärjestelyt, käyttöoikeudet sekä minkälaista tietoa heillä on oikeus saada ja kuinka tieto tulisi suojata.

4.1 Suojautuminen henkilöstön aiheuttamilta vahingoilta

Yritys voi ennaltaehkäistä henkilöstöturvallisuudesta aiheutuvia tahallisia tai ei-tahattomia vahinkoja huolellisilla taustaselvityksillä, lokeroimalla ja luokittelemalla tietoa, ohjeistamalla, kouluttamalla ja kehittämällä yrityksen vallitsevaa henkilöstöpolitiikkaa sekä suunnittelemalla yrityksessä käytettyjä työprosesseja sekä tiedon käsittelyketjuja sellaisiksi, jotka tukevat ajatusta virheiden ennaltaehkäisystä.

Vahinkojen määrän rajoittamiseksi organisaatio voi hyödyntää Parkerin määrittämiä toimia riskien hallintaan:

- **Välttäminen**, joka tarkoittaa henkilöstön sijoittelun ja toimenpiteiden suunnittelua, organisaation resurssien puitteissa, jotta vahingon todennäköisyys pienenisi.
- **Estäminen** rajoittaa työntekijän liikkumista ja toimintaa.

- **Havaitseminen** pyrkii paljastamaan mahdolliset väärinkäytökset sekä sisältää toimintapiteet joilla tiedon väärinkäytökset voidaan estää.
- **Toipuminen** kattaa keinot joilla vahingoista pyritään toipumaan. Vahinko voi olla esimerkiksi tärkeän henkilön kuolemantapaus, äkillinen pitkäaikainen poissaolo tai jokin muu syy joka estää kriittisen työtehtävän suorittamisen.

Jokaiselle työntekijälle tulisi tehdä selväksi hänen vastuunsa työtehtäviinsä liittyvästä tietoturvasta sekä luottamuksellisuudesta. Nämä käsitteet voidaan määritellä jo henkilön työsopimuksessa tai erikseen allekirjoitettavalla salassapitosopimuksella. Organisaatioon saapuvat uudet työntekijät perehdytetään talon tavoille ja toimimaan tietoturvaperiaatteiden mukaisesti. Heille annetaan myös työtehtäviä vastaavat tiedon käyttö- ja saantioikeudet.

Turvallisuuden kannalta kriittiset työtehtävät jaetaan eri henkilöille, työtehtäviä ei siis kahdenneta vaan nimenomaan jaetaan henkilöiden kesken jolloin väärinkäytösten riski pienenee. Tämä vaatii myös kriittisten työtehtävien tarkan dokumentoinnin niin, että mahdollisissa sijaistapauksissa tai toimihenkilön vaihduttua työ voidaan edelleen suorittaa.

Käyttöoikeudet suunnitellaan henkilön työtehtävien, ei organisaatioaseman mukaan. Yrityksen pääjohtajankaan ei tarvitse päästä käsiksi esimerkiksi dokumentteihin yrityksen verkon rakenteesta, käytetyistä ip-osoitteista ja niin edelleen.

Henkilöstön tiedon käyttöä tulisi myös valvoa sekä tallentaa lokitiedostoihin mahdollisten väärinkäytösten havaitsemiseksi ja selvittämiseksi. Tämä voidaan toteuttaa yrityksen toimitiloissa esimerkiksi valvontakameroin ja tietojärjestelmissä lokitiedostoin.

Yrityksen tulee varautua henkilöiden työsuhteiden päättymiseen ja toimiin irtisanoutumisen yhteydessä. Irtisanoutuneen työntekijän tulee palauttaa kaikki hänelle luovutetut avaimet, henkilötunnisteet sekä henkilökortin joka hävitetään asianmukaisesti. Samoin kaikki hänelle annetut tietojärjestelmän käyttäjätunnukset sekä tiedon käyttö- ja saantioikeudet poistetaan. On myös mahdollista tarkistaa onko henkilön tiedon käyttöhistoriassa jotain tavallisuudesta poikkeavaa mahdollisten väärinkäytösten selvittämiseksi. Irtisanoutunut henkilö tulisi myös saattaa toimipistelleen, josta hän valvotusti kerää kaiken henkilökohtaisen omaisuutensa ja jonka jälkeen hänet saatetaan pois organisaation toimitiloista.

4.2 Sosiaalisen median tietoturva

Sosiaalinen media kasvattaa suosiotaan päivä päivältä. Facebook, Twitter, YouTube ja muiden sosiaalisen median sovellusten seuraaminen vie yhä enemmän aikaa. Niistä voi olla organisaatiolle hyötyä, mutta myös haittaa. Organisaation on hyvä näkyä siellä missä asiakkaatkin ovat, mutta toisaalta sosiaalisen median käyttö nostaa esiin pari tietoturvan kannalta tärkeää kysymystä.

4.2.1 Sosiaalisen median uhkakuvat

Yksi merkittävimmistä sosiaalisen median palveluiden tietoturvallisuuden uhkakuvista on muun kuin julkisen tietoaineiston paljastuminen tai joutuminen väärin käsiin. Käyttäjä itse saattaa vuotaa luottamuksellista tietoa tietämättään tai vahingossa. Käyttäjä saattaa päivittää tietoja eri palveluihin jolloin niistä voidaan laatia mahdollisesti vahingollista tai luottamuksellista materiaalia, esimerkiksi käyttäjän ystävä, työtoveri, tai puoliso tiedostamattaan julkaisee kuvia, jotka paljastavat salassapidettäviä tietoja. (Valtiovarainministeriö 2010, 13 - 14).

Käyttäjien sosiaalisessa mediassa käyttämät käyttäjätunnukset voivat joutua varkauden uhriksi, jolloin varas voi saada käsiinsä arkaluontoista tietoa, mustamaalata yrityksen maineen, julkistaa väärää tietoa jne.

Käytettäessä sosiaalisen median palveluita tulisi pitää mielessä myös identiteettivarkauden riski. Käyttäjän tulisi huolellisesti miettiä minkälaista tietoa itsestään ja läheisistään hän palveluun haluaa jakaa. Jaettaessa paljon yksityiskohtaista tietoa voi epärehellinen käyttäjä muodostaa melko tarkan kuvan toisen käyttäjän identiteetistä ja käyttää sitä väärin jossakin toisessa palvelussa.

Koska organisaatioiden henkilöstö usein käyttää sosiaalisen median palveluita,voi yhdenkin henkilön toiminta aiheuttaa riskejä sekä henkilölle itselleen sekä myös organisaation tietoturvallisuudelle. Erityisesti tietojen kalastelu on muodostunut merkittäväksi ongelmaksi. Käyttäjiä yritetään huijata paljastamaan tietoja itsestään tai työnantajastaan aidolta näyttävillä kyselyillä (Valtiovarainministeriö 2010, 15). Tietojenkalastelutapaukset saattaa tunnistaa mm. kielioppi- sekä kirjoitusvirheistä.

4.2.2 Tekniset uhat sosiaalisessa mediassa

Merkittävimmät tekniset uhat ovat sovellushaavoittuvuudet, haittaohjelmat sekä roskapostit. Monet sekä palvelin- (server) että työasema- (client) sovellukset sisältävät haavoittuvuuksia, jotka mahdollistavat esim. käyttäjän koneen haltuunoton, haittaohjelmien levittämisen tai käyttäjän ohjaamisen saastuneille sivustoille (Valtiovarainministeriö 2010, 16).

Haittaohjelmien levitys on käynyt helpommaksi sosiaalisen median kasvun myötä. Käyttäjät suhtautuvat ystäviltään tuleviin linkkeihin paljon luottavaisemmin kuin esimerkiksi tuntemattoman sähköpostin mukana saapuneeseen linkkiin. Tämä altistaa käyttäjän koneen haittaohjelmille. Uudet www-selaimessa käytettävät ja paljon suoritettavaa koodia sisältävät palvelut kuten Facebook, Twitter ja YouTube sisältävät paljon enemmän haittaohjelmia kuin vanhemmat sosiaalisen median muodot, kuten keskustelulaudat ja -foorumit.

Yhdysvaltalaisen Panda Securityn heinäkuussa 2010 suorittaman tutkimuksen mukaan noin kolmannes pienistä ja keskisuurista yrityksistä Yhdysvalloissa on joutunut sosiaalisen median kautta levinneiden haittaohjelmien uhriksi. Noin 35 % näistä yrityksistä on kärsinyt rahallisia menetyksiä, joista kolmannes on ollut yli 5 000 dollaria. (Panda Security 2010, 3).

Sosiaalisen median avustuksella roskapostitusten kohdentaminen on muuttunut entistä helpommaksi. Roskaposteja voidaan kohdentaa mm. erilaisten ryhmien tai suosittujen sivustojen mukaan. Roskapostituksen estäminen onkin nykyään erittäin hankalaa, sillä roskapostittajat yleensä vain vaihtavat toimimattomat osoitteensa uusiin ja jatkavat roskapostin lähetystä.

Kuten henkilöstöturvallisuudessa yleensä, voidaan sosiaalisen median muodostamia uhkia turvata koulutuksella ja käyttöohjeilla. Käytettäessä sosiaalisen median palveluita organisaation teknisillä laitteilla tulisi ne suojata asianmukaisin keinoin.

5 TIEDON TIETOTURVA

Tiedon tietoturva tarkoittaa organisaatiossa olevan tiedon suojaamista esimerkiksi virustorjuntaohjelmistoin, varmuuskopioinnein.

Kaikki tietotekniset laitteet tulisi suojata vähintäänkin salasanoin. Hyvä salasana on sellainen, joka ei ole arvattavissa ja sisältää kirjaimia, numeroita sekä erikoismerkkejä. Jos salasana on liian helppo se on murrettavissa joko päättelemällä tai käyttäen murtamiseen suunniteltua työkalua minkä jälkeen hakkeri pääsee käsiksi laitteessa oleviin tietoihin. Liian vaikea salasana on taas vaikea muistaa ja pahimmassa tapauksessa laite joudutaan alustamaan salasanan nollaamiseksi siten, että tietoja ei saada varmuuskopioitua.

Oikea paikka salasanoille ei ole post-it -lapulla näytön kyljessä tai tekstitiedostossa laitteen muistissa vaan käyttäjän omassa päässä. Samaa salasanaa ei myöskään tulisi käyttää useammassa palvelussa. Tietoturva-aukko yhdessä palvelussa muodostaisi näin riskin muille järjestelmille.

Toimivan salasanapolitiikan lisäksi laitteisiin tulisi asentaa ajantasalla oleva virustentorjuntaohjelmisto. Näin varmistetaan laitteiden suojaus matoja, viruksia sekä troijalaisia vastaan. Käyttäjille tulisi myös painottaa terveen maalaisjärjen käyttöä heidän hoitaessaan asioitaan internetissä. Outojen linkkien sekä sähköpostin liitetiedostojen avaaminen saattaa johtaa laitteen saastumiseen. Älypuhelimiinkin on alkanut ilmaantua viruksia ja matoja. Niihin onkin saatavilla myös mobiilitietoturvasovelluksia. Älypuhelinta työtehtäviin käyttävälle tulisikin hankkia myös asianmukainen tietoturvasovellus laitteen turvaamiseksi.

5.1 Varmuuskopiointi

Varmuuskopioinnilla tarkoitetaan yleensä tapahtumaa, jossa jokin tärkeä tieto kopioidaan ja varastoidaan. Jos alkuperäinen tieto häviää tai tuhoutuu, voidaan tieto palauttaa varmuuskopioista.

Nykypäivänä organisaatioille on tarjolla monia erilaisia tiedonvarmennusratkaisuja. Näitä ovat esimerkiksi optiset tallennusvälineet (cd-, dvd-, bluray-levyt), haihtumattomat muistityypit (flash-muistit), magneettiset tallennusvälineet (kiintolevyt ja magneettinauhat) sekä online-varmuuskopiointi, jossa tieto kopioidaan

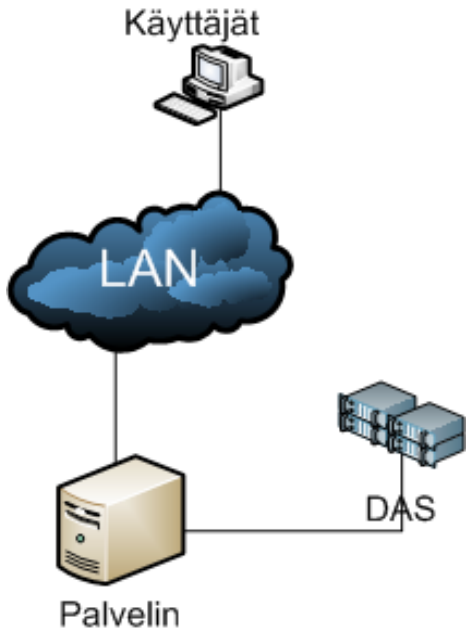
palveluntarjoajan tiedostopalvelimille käyttäen palveluntarjoajan siihen suunnittelemaa ohjelmaa.

Varmuuskopiointiratkaisua suunniteltaessa on hyvä miettiä minkälaista varmennusratkaisua käytetään, kuinka usein varmuuskopiot otetaan ja mitä varmuuskopioidaan. Pienien datamäärien varmuuskopiointiin SAN-ratkaisut ovat yleensä ylilyönti, mutta pienehkö NAS-asema tai online-kopiointi voivat olla hyviä vaihtoehtoja DAS-tyyppisen ratkaisun ohelle.

5.1.1 NAS, SAN ja DAS

NAS, SAN ja DAS ovat tapoja rakentaa organisaation tiedon varmennus- sekä säilytysratkaisu. DAS ja NAS sopivat myös pienorganisaatioille, sillä niiden hankintakustannukset voivat olla yllättävän alhaiset.

DAS on suoraan laitteeseen kytketty tallennusresurssi (kuva 3). DAS-laitetta voidaankin ajatella saarekkeena, jolle on pääsy vain yhdestä paikasta. Tässä piilee myös DAS-laitteiden heikkous, sillä niillä sijaitsevat resurssit ovat vain niissä kiinni olevan laitteen käytettävissä. DAS-laitteita ovat muun muassa nauha-asemat.



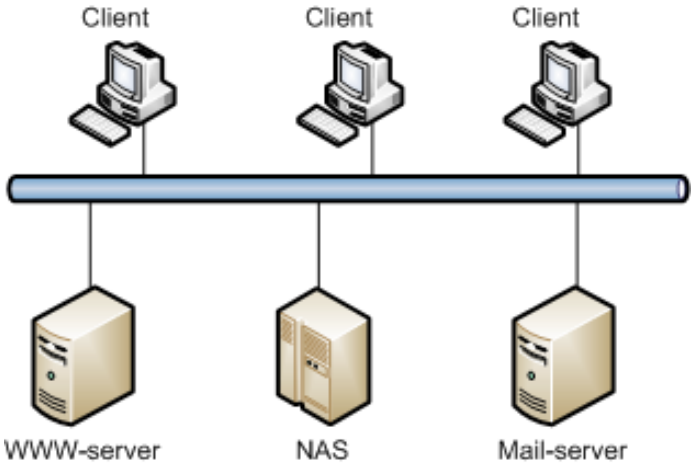
KUVA 3. DAS:n rakenne.

NAS on verkossa sijaitseva palvelin, joka toimii tallennusresurssina muille verkon laitteille (kuva 4). Yleensä NAS-palvelimessa on käytössä myös RAID-ominaisuus. RAID kasvattaa laitteen vikasietoisuutta tuomalla käyttöön reduntanttisuudella.

Yrityskäyttöön suunnatuissa NAS-laitteissa on myös yleensä tuplatut verkkoliitännät joko vikasietoisen verkkoliitynnän tekemiseen tai vaihtoehtoisesti ns. NAS-to-NAS-ratkaisun luomiseen mikä liittää kaksi samanlaista NAS-laitetta toisiinsa ja ne peilaavat datansa keskenään. Yleensä laitteissa on myös USB-liityntä datan peilaamiseen ulkoiselle kiintolevylle.

Tiedonsiirto NAS-järjestelmissä tapahtuu yleensä käyttäen joko NFS- tai CIFS-protokollia. CIFS-protokolla on uusin versio Linuxin käyttämästä Samba-tiedostojenjakoprotokollasta. NAS-palvelin hoitaa itsenäisesti myös käyttäjien autentikoinnin hyväksikäyttäen joko omia luotuja autentikointisääntöjä tai esimerkiksi Windows-palvelinten Active Directory –ominaisuutta, jolloin käyttäjät kirjautuvat NAS-palvelimeen sekä verkkoon samoilla käyttäjätunnuksilla ja salasanoilla. Levyosiot voidaan suojata käyttäen 256-bittistä AES-salausta, joka on tällä hetkellä ainoa murtamaton salausmenetelmä.

NAS-järjestelmät ovat muuttuneet kotikäytössä yhä suositummiksi kiintolevyjen halpenemisen myötä. Monet käyttäjät ovat valjastaneet vanhoja koneitaan NAS-palvelimiksi kotiverkkoonsa. NAS-järjestelmä on siis mahdollista kasata vanhasta, käytöstä poistetusta työasemasta sopivan käyttöjärjestelmän avulla (esim. FreeNAS) tai se voidaan hankkia valmiina. Kaupalliset NAS-ratkaisut ovatkin helppokäyttöisiä eivätkä välttämättä vaadi yritykseltä IT-henkilökuntaa niitä huoltamaan. Suurimpina kaupallisten NAS-järjestelmien valmistajina voidaan mainita Dell ja Hewlett Packard.



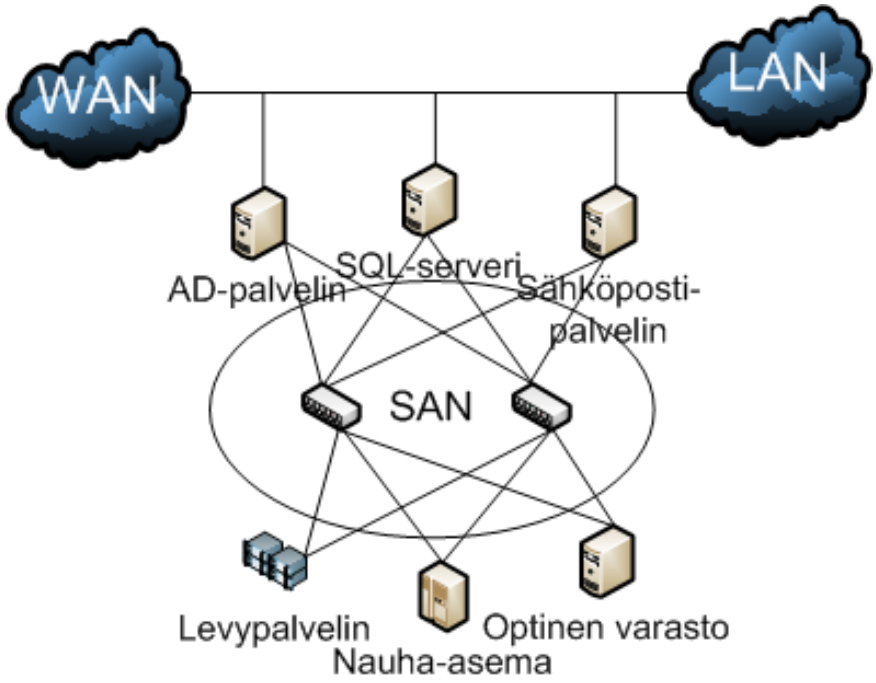
KUVA 4. NAS:n rakenne.

NAS-laitteilla on myös muuta käyttöä kuin vain mahdollinen tiedostojen jako sekä varmuuskopiointiratkaisuna toimiminen. Nykyään niissä on mahdollisuus toimia kodin tai organisaation "viihde"keskuksina. Ne osaavat striimata videota nettiin sekä toimia

vaikkapa BitTorrent-clientteinä. Myös Microsoftin uudesta Windows Home Server -käyttöjärjestelmästä löytyy mahdollisuus toimia NAS-palvelimena.

SAN eli tallennusverkko (kuva 5) on suunniteltu tiedon tallennukseen. SAN on oma eriytetty verkko, joka keskittää hajautetut levyjärjestelmät yhteiskäyttöä varten. Järjestelmänä SAN soveltuu parhaiten suuria tietomääriä käsitteleviin keskitettyihin tietovarastoratkaisuihin (Tenhunen 2008, 23).

SANiin voi olla liitettyinä nauha-asemia, levypalvelimia tai optisia kirjastoja. Siirtotienä SAN-verkoissa käytetään yleensä nopeita kuituyhteyksiä riittävän siirtokapasiteetin varmistamiseksi.



KUVA 5. SAN-verkon rakenne.

5.1.2 Online-varmuuskopiointi

Online-varmuuskopioinnissa tieto, joka sijaitsee käyttäjän työasemalla, kannettavalla tai vaikkapa älypuhelimessa, kopioidaan internetin yli palveluntarjoajan tiedostopalvelimille. Tämä tarjoaa pienille yrityksille hyvän tavan hajauttaa varmuuskopiointia ja lisätä näin tietoturvaa. Tietojen kopiointi tapahtuu yleensä eräajona päivittäin. Käyttäjä yleensä asentaa palveluntarjoajan laatiman ohjelmiston työasemalleen, joka hoitaa tiedostojen kopioinnin. Ohjelmistot voivat mahdollisesti tarkkailla siirrossa tapahtuvia virheitä erilaisin tarkistusmenetelmin. Kopioitava data yleensä pakataan sekä lähetys palveluntarjoajan palvelimille suojataan käyttäen SSL-salausta, näin varmistetaan tiedon väärinkäytön estäminen.

Haittana online-varmuuskopioinnissa voidaan pitää palvelun muodostamaa kulua ja mahdollisia siirtovirheitä. Siirtovirheen sattuessa data ei olekkaan enää käytettävissä, mutta yleensä tämä ongelma on ratkaistu palveluntarjoajan ohjelmistossa. Yrityspalvelut ovat yleensä vuosihinnoiteltuja ja hinta kasvaa datamäärän kasvaessa. Samoin palvelun pysyvyys voi muodostaa ongelman. Osa alan toimijoista onkin lopettanut palvelunsa kannattamattomina, esimerkiksi HP lopetti "Upline" -varmuuskopiointipalvelunsa vuonna 2009 vain noin vuoden toiminnan jälkeen.

5.1.3 FreeNAS

FreeNAS on ilmainen FreeBSD:hen perustuva käyttöjärjestelmä. FreeNAS:lla voidaan siis muuntaa tietokone verkkotallennuslaitteeksi. FreeNAS:n voi ladata itselleen osoitteesta freenas.org.

Toimiakseen FreeNAS ei tarvitse kovin tehokasta konetta. Toki koneen laskentakyky vaikuttaa esimerkiksi tiedonsiirtonopeuksiin nopeissa lähiverkoissa. Järjestelmän kehittäjien suosittelemat vähittäisvaatimukset FreeNAS:a pyörittävälle koneelle ovat:

- Vähintään 192Mb RAM, sulautetuissa järjestelmissä 256Mb, sekä jokin seuraavista;
- Levykeasema konfiguraatioiden tallentamista varten ja kiintolevy(jä) tiedon tallentamista varten
- Boottaava USB- tai CF-asema sekä kiintolevyjä
- Boottaava kiintolevy sekä muita kiintolevyjä
- Tai jokin virtuaalinen ympäristö, esim. VmWare

Ominaisuuksiltaan FreeNAS on todella kattava. Tuettuja verkkoprotokollia tiedonsiirtoon on paljon, mm: FTP, SMB/CIFS, TFTP ja niin edelleen. Kiintolevyjen hallintaan on tuki Sun Microsystemsin kehittämälle erittäin tehokkaalle ZFS-levyjärjestelmälle sekä FreeNAS tukee monia tunnettuja levynallokointimenetelmiä mm. Windowsin käyttämät NTFS / FAT sekä Linuxin ext2/3. Siitä löytyy myös mm. ominaisuus sähköpostivaroituksiin, syslog-ominaisuudet, tuki erilaisille UPS-järjestelmien käyttämille ominaisuuksille, web-serveri, BitTorrent-client, iTunes/DAAP-ominaisuus ja monia muita.

FreeNAS onkin varteenotettava vaihtoehto monille kaupallisille NAS-ratkaisuille. Pystyttäminen vaatii toki jonkinlaista tietämystä sekä tottakai käytettävän laitteiston, mutta tarjoaa vastineeksi todella laajat ominaisuudet ja erittäin halvan hinnan.

5.1.4 RAID

RAID, eli Redundant Array of Independent Disks, on tapa jolla laitteessa olevat erilliset kiintolevyt voidaan yhdistää yhdeksi loogiseksi asemaksi. Tämä kasvattaa järjestelmän vikasietoisuutta sekä joissain tapauksissa nopeuttaa järjestelmää. Järjestelmän nopeutuminen perustuu lukunopeuden kasvuun. RAID-tasoja on olemassa monia, mutta yleensä puhutaan tasoista 0, 1 sekä 5.

RAID0 eli lomitus (striping) on tekniikka jolla *n* määrä *c* kokoisia levyjä voidaan yhdistää yhdeksi loogiseksi asemaksi. Tällöin saavutetaan *n* * *c* kokoinen tallennustila. Luku- sekä kirjoitusnopeus RAID0-pakassa on myöskin *n*-kertainen. Data kirjoitetaan lomittain levyille, eli sitä ei kahdenneta tai pariteettidataa ei oteta talteen. Tämä tarkoittaa sitä, että yhdenkin levyn hajotessa kaikki tieto RAID0-pakassa menetetään.

RAID1 eli peilaus (mirroring) on tapa jolloin tallennettava data peilataan kahdelle (tai useammalle) levylle. Tällöin yhden levyn hajotessa data säästyy. Periaatteessa RAID1 kaksinkertaistaa pakan lukunopeuden

RAID5 pitää sisällään pariteettidatan tallennuksen. Se tuo käyttöön *c* * (*n – 1)* kokoisen tallennustilan, jossa *c* on yhden levyn kapasiteetti ja *n* levyjen määrä. Yhden levyn kapasiteetti käytetään juurikin pariteettidatan tallentamiseen ja pariteettidata hajautetaan jokaiselle levylle. Näin varmistetaan se, että mikä tahansa levy RAID5-pakasta hajotessaan ei vaikuta pakan toimivuuteen. Useamman, kuin yhden levyn samanaikainen vikaantuminen hävittää myöskin pakan kaiken datan. RAID5-ominaisuutta voidaan käyttää myös ilman pariteettidataa, mutta tällöin menetetään kaikki vikasietoisuuden tuomat edut. Luku- sekä kirjoitusnopeus kasvaa jonkinverran, mutta pariteettidatan vuoksi RAID5 tarvitsee laitteelta paljon laskentatehoa. RAID6 toimii periaatteessa samoin, kuin RAID5, mutta pariteettidatan tallennukseen on varattu enemmän tilaa. RAID6 pakasta voikin hajota 2 levyä ennenkuin data menetetään.

RAID-tasoja voidaan myös yhdistää. Esimerkiksi RAID0+1 yhdistää peilauksen sekä lomituksen. Tällöin luku-, kirjoitusnopeus sekä vikasietoisuus kasvavat. Data RAID0+1-pakassa on palautettavissa, jos peilissä on yksi ehjä levy.

5.2 Virustorjunta

Nykypäivänä viruksia, troijalaisia sekä matoja liikkuu internetissä tavattoman paljon. Osa näistä ohjelmista on erittäin tuhoisia, kuten esimerkiksi vuonna 2010 riehunut Stuxnet-niminen mato, joka pystyi jopa hyökkäämään teollisuuslaitosten automaatiojärjestelmien kimppuun ja näin aikaansaamaan mittavaakin vahinkoa.

Viruksien, matojen ja troijalaisten toimintaperiaatteet eroavat hiukan toisistaan. Virukset, jotka luetaan yleensä haittaohjelmistoihin, vaatii aina käyttäjän toimia, jotta se voisi tarttua laitteistoon. Esimerkiksi jonkin tiedoston avaaminen voi tartuttaa laitteistoon viruksen.

Myös madot luetaan haittaohjelmistoiksi, mutta ne eivät vaadi käyttäjän tai isäntäohjelmistolta toimia levitäkseen. Madot leviävät yleensä internetin välityksellä, ja ne käyttävät hyödykseen järjestelmistä löytyviä tietoturva-aukkoja. Oppivia madot eivät kuitenkaan ole, joten tietoturva-aukon tukkiminen estää madon pääsyn koneelle. Mahdollisuus toki on, että mato pääsee koneelle jotakin toista kautta, esimerkiksi saastuneelta ulkoiselta kiintolevyltä.

Troijalainen tai Troijan hevonen on harmittomaksi ohjelmaksi, koodinpätkäksi tai tiedostoksi naamioitunut haittaohjelma. Avattaessa tiedosto, ohjelma tai ajettaessa koodinpätkä haittaohjelma aktivoituu ja saastuttaa järjestelmän. Troijalainen voi pitää sisällään viruksen tai madon tai se voi aukaista esimerkiksi käyttäjän tietämättä jonkin tietokoneen portin ulkoverkkoon ja täten luoda tietoturva-aukon järjestelmään.

Lukumääräisesti eniten viruksia on tietenkin Microsoftin käyttöjärjestelmille, joista käytetyin on edelleen Windows XP. Sille on myös lukumääräisesti eniten viruksia. Microsoftin uutta Windows 7 -käyttöjärjestelmää pidetään edeltäjäänsä Vistaa luotettavampana, mutta se ei ole läheskään niin suosittu käyttöjärjestelmä kuin Windows XP. Macintosh- ja Linux-käyttäjät ovat vielä suhteellisen turvassa viruksilta, mutta näillekkin käyttöjärjestelmille niitäon alkanut esiintyä. Mobiililaitteiden yleistyessä myös haittaohjelmat tulevat lisääntymään. Älypuhelinkin olisi hyvä suojata virustorjuntaohjelmistoin.

Hyvä palomuuri toki poistaa osan haittaohjelmien aiheuttamista ongelmista, mutta virustorjuntaohjelmiston tärkeyttä ei koskaan voida korostaa liikaa. Virustorjuntaohjelmistoja on niin ikään maksullisia sekä maksuttomia. Maksullisista voidaan mainita suomalainen F-Secure sekä vaikkapa Norton. Maksuttomista virustorjuntaohjelmistoista hyväksi on osoittautunut Avast!-merkkinen ohjelmisto. Microsoftin Windows 7 -käyttöjärjestelmän omistajat saavat ladata ilmaiseksi Microsoft Security Essentials -nimisen tuotteen, joka suojaa koneen reaaliaikaisesti viruksilta, vakoiluohjelmistoilta sekä muilta haittaohjelmistoilta.

5.3 Tiedon tuhoaminen

Tiedon tuhoaminen on tärkeää organisaation tietoturvan kannalta. Esimerkiksi käytöstä poistetut muistitikut, tietokoneet, cd- ja dvd-levyt sisältävät tietoa, joka voi vahingoittaa yritystä. Myöskään organisaation papereita ei koskaan tulisi heittää roskiin sellaisenaan vaan ne tulisi aina tuhota ennen poisheittämistä.

Työasemien kiintolevyt voidaan poisheitettäessä tuhota tehokkaasti voimakkaalla magneetilla. Kiintolevyn toimintaperiaatteen vuoksi ulkopuolinen magneettikenttä demagnetoi kiintolevyn levypakat ja aiheuttaa sen, että kiintolevy on käyttökelvoton. Samoin käytöstä poistettava kiintolevy voidaan hajoittaa fyysisesti, ja se ei enää aiheuta tietoturvauhkaa. Näitä menetelmiä sovellettaessa on otettava huomioon se, että laitetta ei enää toimenpiteiden jälkeen voi käyttää, vaan se on käyttökelvoton.

Ulkopuoliset palveluntarjoajat tarjoavat myös palveluita tiedon hävittämiseen. Palvelut perustuvat yleensä tiedon ylikirjoittamiseen. Levyn sisältö tyhjennetään ja sille kirjoitetaan uutta dataa vanhan tiedon piilottamiseksi. Periaatteessa yksi ylikirjoituskerta riittää datan hävittämiseksi. Yleisenä standardina kuitenkin pidetään sitä, että levy tulisi ylikirjoittaa vähintään seitsemän kertaa, ennen kuin alkuperäisen tiedon voidaan olettaa olevan lukukelvotonta. Yritys- ja kotikäyttöön soveltuvaa ylikirjoitusohjelmaa markkinoi muunmuassa Blancco. Ylikirjoittamisen hyvä puoli on se, että kiintolevy on toimenpiteen jälkeen täysin toimintakelpoinen ja PC voidaan voidaan kierrättää joko myymällä, lahjoittamalla tai jollain muulla tavalla.

Paperia, cd- ja dvd-levyjä varten organisaatioon voidaan hankkia tarpeeksi tehokas asiakirjasilppuri. Silppureiden tuhoamiskyvyssä on eroja. Jokapäiväisten, harmitonta tietoa sisältävien asiakirjojen tuhomiseen riittää kategorian 1 silppuri, jonka muodostaman silpun suikaleleveys on 12 mm. Erittäin salaisille asiakirjoille suositellaan kategorian 5 tai 6 silppuria, jonka silpun suikaleveys on alle 1 mm ja pituus 5 mm. Nykypäivänä silppureilla on myös mahdollista tuhota optisia levyjä.

6 LAITTEISTO- JA FYYSINEN TURVALLISUUS

Fyysinen turvallisuus jaetaan yleisesti laitteiden turvallisuuteen sekä organisaation toimitilojen turvallisuuteen. Yleinen käsitys tietoturvasta on se, että sillä tarkoitetaan tietoliikennelaitteiden sekä tietokoneiden suojaamista luvattomalta käytöltä, mutta toimitilojen turvallisuudella on myös tärkeä rooli toimivassa tietoturvassa.

6.1 Laitteistoturvallisuus

Laitteistoturvallisuus tarkoittaa tietoverkon laitteiden, palvelinten, työasemien sekä muiden tietoteknisten laitteiden fyysistä turvaamista. Näitä laitteita voivat olla esimerkiksi verkkotulostimet ja älypuhelimet.

Mikäli mahdollista, kaikki tietotekniset laitteet tulisi lukita johonkin kiinteään niiden varastamisen estämiseksi tai ainakin vaikeuttamiseksi. Samoin ulkoiset kiintolevyt, muistitikut, cd- tai dvd-levyt, jne tulisi säilyttää lukittujen ovien takana silloin, kun niitä ei käytetä jolloin niiden riski niiden joutumisesta vääriin käsiin pienenee huomattavasti.

Laitteissa käytettyjen kaapeleiden liityntäpisteet tulisi suunnitella siten, että ne ovat poissa henkilöiden tieltä. Tällöin varmistetaan se, että kukaan ei kompastu kaapeleihin tai vaikkapa siivoaja ei vahingossa repäise palvelimen virtajohtoa irti.

Organisaation tulisi varautua myös sen ulkopuolisiin, mutta siihen vaikuttaviin tapahtumiin, esimerkiksi sähkökatkoihin. Nykyään on saatavilla UPS-järjestelmiä, jotka tarjoavat sähköä niihin kytkettyihin laitteisiin lyhyiden (minuuttiluokan) katkosten aikana. Yleensä UPS-järjestelmiin liitetään ohjelmisto, joka ajaa niihin kytketyt laitteet hallitusti alas, jolloin tietoja ei menetetä sähkökatkon sattuessa. Organisaation palvelimet tulisi suojata ainakin UPS-järjestelmällä. UPS-järjestelmien hyvänä puolena mainittakoon myös niiden kyky tasoittaa sähköverkossa sattuneita jännitepiikkejä, jotka voivat myös rikkoa sähkölaitteita sekä kyky tasoittaa sähkönlaatua.

Laitetilassa olevat 19”-laiteräkit tulisi varustaa vähintään kaksiosaisella maadoitetulla pistorasialla joihin on mahdollista liittää räkkiasennusta varten suunniteltuja pistorasiapaneeleita. Räkkiasennetun pistorasian tulee olla omassa sähkönsyöttöryhmässään.

Lämpimän ilman poisto tulisi tehdä laiteräkkien vastakkaiselta puolelta ja laiteräkkeihin tulisi asentaa tuuletin. Tuuletin voidaan asentaa joko räkin ylä- tai alaosaan.

6.2 Kannettavien laitteiden ja älypuhelinten tietoturva

Organisaation kannettavat laitteet sekä työntekijöillä mahdollisesti käytössä olevat älypuhelimet (iPhone, Android, Symbian...) tulisi myös turvata uhkien varalta.

Kannettavien tietokoneiden turvaamiseen soveltuvat samat säännöt kuin työasemienkin, mutta lisäksi niiden sisältö tulisi salakirjoittaa, eli kryptata. Tällöin varmistetaan se, että varkaus- tai katoamistapauksessa laitteen sisältämä tieto ei joudu ulkopuolisten käsiin.

Älypuhelimet valtaavat nykypäivänä markkinoita huimaavalla vauhdilla. Ei olekkaan yllätyksellistä, että niille on myös alkanut esiintyä haittaohjelmia ja viruksia. Suojautuminen näiltä ei kuitenkaan vaadi korkeakoulututkintoa vaan niiltä voidaan suojautua melko helposti.

Puhelimen ja siihen hankittujen ohjelmistojen tulisi aina olla ajan tasalla. Käyttöjärjestelmän ja ohjelmistojen mahdollista automaattista päivitystä tulisi käyttää. Laitteeseen tulisi hankkia myös virustentorjuntaohjelmisto, joko maksullinen (esim. F-Secure tai McAfee) tai maksuton (esimerkiksi AVG AntiVirus). Puhelimen verkonkäyttöä tulee myös rajoittaa. Tällä tarkoitetaan sitä, että Bluetoothin ja langattomien verkkojen käyttö ei ole automaattista vaan tapahtuu vain käyttäjän niin halutessa. Samoin langattomia verkkoja käytettäessä tulisi käyttää vain tunnettuja, suojattuja ja luotettavia verkkoja. Muina aikoina nämä ominaisuudet voidaan kytkeä pois päältä.

Suojaa laitteesi hyvällä PIN-koodilla. Jos laitteessa on mahdollisuus suojata näytönsäästäjä jollakin tavalla (esim. Android-puhelimissa tähän voidaan käyttää joko PIN-numeroa, erillistä salasanaa tai kuvioon perustuvaa todennusta.) tulisi se ottaa käyttöön.

Laitteen sisällöstä tulisi ottaa varmuuskopio tasaisin väliajoin sekä sen sisältö tulisi myös kryptata. Katomistapausten varalle laitteen takakanteen voidaan liimata omistajan yhteystiedot sen varalle, jos puhelimen löytäjä onkin hyväsydäminen henkilö. Yhteystietoihin kannattaa lisätä esimerkiksi varaliittymän tai työnantajan yleinen puhelinnumero. Joihinkin puhelimiin on saatavilla myös pc:llä käytettäviä

etähallintaohjelmistoja, esim HTC:n valmistamiin puhelimiin HTC Sense, Applen iPhonelle MobileMe sekä Windows Mobile -puhelinten Live ID -palvelu. Maksullisina verrokkeina voidaan mainita McAfeen WaveSecure. Varkaudenhallintaohjelmista antaa käyttäjälle mm. mahdollisuuden poistaa puhelimesta tietoja, estää käyttöjärjestelmän osien (esim. kalenteri) luvatonta käyttöä tai estää puhelimessa olevien tietojen kuten sms- tai sähköpostiviestien lukemista. Laitteesta luovuttaessa, tulisi kaikki tieto poistaa laitteesta asianmukaisesti (Fried 2010, 197).

6.3 Fyysinen turvallisuus

Fyysinen turvallisuus tarkoittaa toimitilojen turvaamista ulkoisilta uhilta. Näitä ovat esimerkiksi tulipalo, luvattomat vierailijat sekä vesivahingot.

Laitteiden ja tietojärjestelmän nerokkaat suojaukset eivät auta sellaista hakkeria tai epärehellistä käyttäjää kohtaan, joka pääsee laitteeseen fyysisesti käsiksi tai pahimmassa tapauksessa voi viedä sen jopa mukanaan pois organisaation tiloista. Esimerkiksi elektroninen kulunvalvontajärjestelmä voidaan yhdistää muuhun tietojärjestelmään vaikkapa siten, että käyttäjä ei pääse kirjautumaan intranetin tietokoneille, ellei hän ole kulunvalvontajärjestelmän mukaan sisällä yrityksen tiloissa. Vastaavasti käyttäjän ei tarvitse pystyä avaamaan VPN-yhteyttä intranetiin, jos hän on sisällä yrityksen tiloissa (Ruohonen 2002, 5).

6.3.1 Kameravalvonta

Kameravalvonta, kulunvalvonnan yhteyteen liitettynä, on myös erittäin tehokas tapa ehkäistä laitteiden väärinkäyttöä. Todellista varastahan kameravalvonta ei tietenkään pelota, mutta epärehellinen käyttäjä miettii tekojaan varmasti kerran jos toisenkin. Tallentavan kameravalvonnan yhteydessä tulisi ottaa myös huomioon erinäiset lakitekniset asiat. (Asetuksia työpaikalla tapahtuvaan kameravalvontaan).

6.3.2 Tulipalo

Tulipalo on yksi vaarallisimmista asioista mikä yritystä voi kohdata. Tulipalovaaran takia varmuuskopioita ei tulisi säilyttää organisaation tiloissa. Aina tämä ei tietenkään ole mahdollista, jolloin tulisi varmistaa, että varmuuskopioita on sellainen määrä ja ne

sijaitsevat eri puolilla toimitiloja sekä toivoa, että ne kaikki eivät tuhoudu tulipalossa. Organisaatioon voidaan toki hankkia myös pieni paloturvallinen mediakaappi, jossa kaikkein tuoreimpia varmuuskopioita säilytetään. Mediakaappeja on saatavilla erilaisin turvallisuusluokituksin, parhaimmillaan ne säilyttävät sisältönsä jopa 60min koskemattomina.

Tulipaloon voidaan toki varautua. Alkusammutuskaluston sijainti on merkittävä selvästi ja sen kuntoa on seurattava säännöllisin tarkastuksin. ICT-laitetila tulisi aina myös varustaa jonkinnäköisellä palonilmaisinjärjestelmällä (Valtiovarainministeriö 2002, 10 - 11).

Erilaiset automaattiset sammutusjärjestelmät, joko normaalit sprinklerityyppiset tai kaasupohjaiset, ovat hyviä torjuttaessa tulipaloja. EN-1047-2 -rakennusstandardi kertoo ICT-laitetilalta vaadittavat paloturvallisuusvaatimukset. Pienillä yrityksillä tosin ei aina ole varaa hankkia standardien mukaisia laitetiloja niiden korkeiden kustannusten takia. Normaalia sprinklerityyppistä järjestelmää ei sen toimintaperiaatteen takia kannata laitetilaan laittaa, sillä vesi ja sähkö ovat tunnetusti huono yhdistelmä.

6.4 Vesivahinko

Yrityksen tiloissa tapahtuva vesivahinko voi myös aiheuttaa tietojen menetystä. Sähkölaitteiden ja veden yhteensopivuuden kaikki tunnetusti tietävät, mutta samoin vedestä kärsii myös paperilla oleva tieto. Varsinkin, jos altistuminen vedelle on pitkäaikaista tai vesimäärät ovat suuria voi paperitieto muuttua pahimmillaan lukukelvottomaksi. Sähköiseltä medialta tieto on yleensä palautettavissa vesivahingon jälkeen, sillä vesi ei niinkään muuta kiintolevyn magnetointia vaan vaikuttaa sen sähköosien toimivuuteen. Asiansa osaava tietoturva-alan yritys kyllä saa tiedot palautettua myös vesivahingon kärsineiltä kiintolevyiltä.

Vesivahingolta suojautumiseksi tulisi huomioida se, missä vesiputket kyseessä olevissa tiloissa kulkevat. ICT-tilat voidaan tällöin suunnitella kauemmas olemassa olevista vesiputkista, jotka rikkoontuessaan saattavat aiheuttaa mittaviakin vahinkoja. Uusia toimitiloja rakennettaessa ei vesiputkistoja tulisi suunnitella laitetilan läheisyyteen. Samoin tulisi ottaa huomioon mahdolliset luonnon aiheuttamat ja mahdolliseen vesivahinkoon johtavat tapahtumat. Näitä ovat esimerkiksi tulvat sekä rankkasateet. ICT-tila tulisi vähintäänkin varustaa hyllyin, mieluummin toki 19"-räkein joihin laitteet asennetaan. Esimerkiksi varastotiloissa suositellaan tavaroiden

nostamista lastauslavan verran lattiatason yläpuolelle. ICT-tiloissa tulisi kuitenkin suosia korkeampia korkeuksia varmuuden välttämiseksi. Paras ratkaisu toki olisi räkkiasennetut laitteet sekä korotettu lattia.

7 TIETOVERKON TIETOTURVA

Ennen verkon suojaamisen yksityiskohtaista suunnittelemista, on mietittävä verkon rakenne: minkälaisiin segmentteihin tai aliverkkoihin palvelut sijoitetaan, mitä kaapelointijärjestelmiä ja verkon aktiivilaitteita käytetään sekä minkälaisia laajaverkkoliittymiä hankitaan (Hakala, Vainio 2005, 344).

Hankittavia aktiivilaitteita yleensä ovat; palomuuri, reititin/reitittimet sekä kytkimet, joissakin verkoissa saatetaan tarvita toistimia taikka siltoja, mutta näitä harvemmin enää tapaa.

Suunnittelussa tulee ottaa myös huomioon käytetyt IP-osoiteavaruudet, mahdolliset VPN-yhteydet etätyöskentelyä varten, käytetäänkö verkossa nk. DMZ-aluetta. DMZ on aliverkko, joka sijaitsee organisaation lähiverkon ulkopuolella ja jonne sijoitetaan toiminnan kannalta sellaiset palvelut, joiden katsotaan olevan riskialttiita hyökkäyksille ja joiden mahdollinen hakkerointi tai palvelun kaatuminen ei vaikeuta organisaation toimintaa. Tällaisia palveluita voivat olla esimerkksi organisaation WWW-palvelin, extranet-palvelin ja vastaanottavan sähköpostin SMTP-palvelin.

7.1 Palomuuri

Palomuuri on käsitteenä mahdollisimman epämääräinen: sillä voidaan tarkoittaa hyvin erityyppisiä laitteita tai ohjelmistoja joiden tehtävänä on estää asiattomien henkilöiden pääsy joko verkkoon tai tiettyyn verkon tarjoamaan palveluun (Hakala, Vainio 2005, 347).

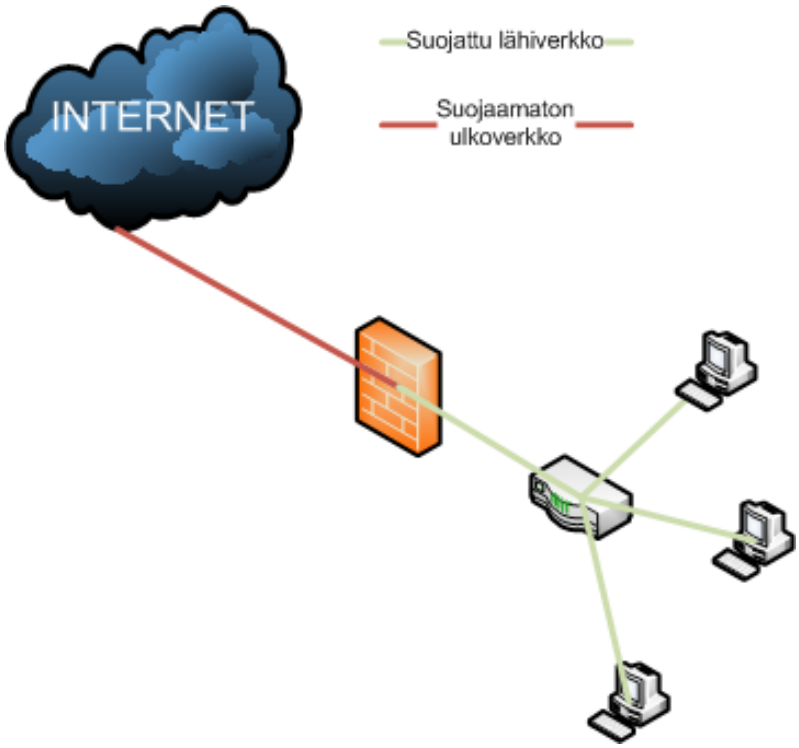
Palomuureja on yleensä kolmea eri perustyyppiä: pakettisuodatteiset, välityspalvelimet sekä sovellustason yhdyskäytävät. Sovellustason yhdyskäytävät ovat näistä kaikkein kehittyneimpiä ja ne vaativatkin toimintaperiaatteestaan johtuen laitteelta suurta laskentatehoja, joka taas näkyy laitteen hankintakustannuksissa.

Palomuurin voi toki rakentaa myös itse. Tarkoitukseen suunnitellut ilmaiset Linux-distribuutiot, kuten IpCop tai m0n0wall ovat kevyitä käyttöjärjestelmiä, jotka toimivat myös vähän vanhemmalla työasemalla. Myös Microsoftin käyttöjärjestelmissä on sisäänrakennettuna palomuuriominaisuus. Tämä ominaisuus oli ensimmäisenä Windows XP –käyttöjärjestelmässä ja se olikin siinä varsin alkeellinen, mutta peruspalomuurina varsin toimiva. Windows XP:ssä ollut palomuuri näet esti ulkoverkosta sisäänpäin tulevan liikenteen eikä siihen esimerkiksi saanut luotua omia

ohjelmakohtaisia sääntöjä. Windows Vistassa sekä uudessa Windows 7 – käyttöjärjestelmässä Windowsin oma palomuuri onkin jo varsin hyvin toimiva kokonaisuus. Nykypäivänä palomuurit tarjoavat myös paljon muita palveluita perustoimintansa lisäksi. Näitä ovat muunmuassa:

- NAT
- VPN
- DHCP
- Liikenteen salaus
- Syslog-palvelut verkkoliikenteen ja pakettien tarkkailuun.

Palomuurin perusperiaatteena on siis estää ei-toivottu liikenne ulkoverkosta sisäverkkoon (kuva 6) joko paketti- tai protokollasuodatukseen perustuen.



KUVA 6. Palomuurin toimintaperiaate.

Palomuurien toiminta perustuu ennalta luotuihin sääntöihin tai niin kutsuttuihin pääsylistoihin. Näissä määritellään joko tiettyjä IP-osoitteita tai kokonaisia osoiteavaruuksia, joista liikenne joko kielletään tai sallitaan. Laajemmissa listoissa voidaan esimerkiksi määritellä vaikkapa käytetty protokolla, kohde- tai lähdeportti (Litmanen 2010, 22).

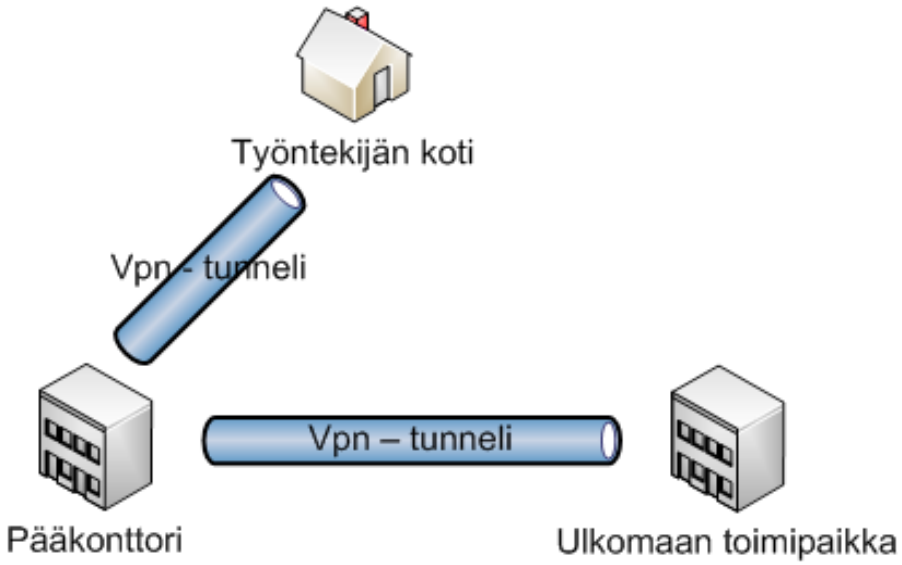
Oletuksena yleensä on, että kaikki liikenne sisäverkosta ulkoverkkoon sallitaan ja ulkoverkon liikenne sisäverkkoon kielletään.

7.2 VPN

VPN:t eli virtuaaliset lähiverkot, ovat tapa muodostaa vahvasti suojattuja etäyhteyksiä yleisen verkon, yleensä internetin, yli organisaation lähiverkon palveluihin.

Alkuaikoina organisaation eri toimipaikat ja osastot kytkettiin toisiinsa käyttäen ns. "leased line"-yhteyksiä, eli palveluntarjoaja luo suoran yhteyden kahden toimipaikan välille tiettyä kuukausikorvausta vastaan. Nykyään kyseinen järjestely voidaan unohtaa VPN-yhteyksien kehityttyä.

Periaatteessa VPN:ää voidaan ajatella tunnelina (kuva 7). Tunnelin päissä sijaitsevat kohteet joiden välille halutaan turvattu yhteys ja paketit näiden kahden kohteen välillä liikkuvat turvatussa, ulkopuolisilta suljetussa, tunnelissa. Tämä järjestely saavutaan luomalla alkuperäisen paketin ympärille toinen, jotakin VPN-protokollaa käyttäen, salattu paketti. Alkuperäinen paketti siis kapseloidaan uuden paketin sisään.



KUVA 7. VPN yksinkertaistettuna.

Alkuperäisen pakein kapselointiin VPN-yhteyksissä käytetään monia erilaisia protokollia. Näitä protokollia ovat mm. GRE, PPTP ja layer 2 forwarding (Hakala, Vainio 2005 382).

7.3 NAT

Network Address Translation, eli lyhyemmin, NAT on palvelu, jossa reititin tai yhdyskäytävä muuttaa sisäverkossa käytettävän IP-osoitteen organisaation rekisteröimään viralliseen IP-osoitteeseen (Hakala, Vainio 2005, 246).

Organisaatioilla on yleensä käytössä monia työasemia, joille tarvitaan IP-osoite. IANA ja kansallisella tasolla jokin teleoperaattoreista, internet-palveluntarjoajista, korkeakoulu tai jokin muu julkinen organisaatio vastaavat ns. julkisten osoitteiden jakamisesta. Suurimpia A- ja B-luokan julkisia osoitesarjoja ei ole enää käytännössä edes saatavilla.

Tämä voidaan kuitenkin ratkaista käyttämällä NAT-palvelua. Tällöin sisäverkossa käytetään joko A-, B- tai C-luokan osoitesarjaa, joka on varattu nimenomaan intranet, eli sisäverkko, käyttöön ja sisäverkosta ulospäin meneviin yhteyksiin sisäverkon IP-osoite korvataan organisaation julkisella osoitteella. Tällöin tarvitaan vain yksi julkinen osoite monen osoitteen sijaan. Tämä säästää kuluja, sillä näin tarvitaan vuokrata vain yksi julkinen osoite sekä ratkaisu nostaa myös tietoturvan tasoa sillä, jos paketti kaapataan ei kaappaaja näe muuta, kuin palomuurin julkisen IP-osoitteen, sisäverkon IP-osoitteet pysyvät näin turvattuina.

7.4 Palomuurin muut palvelut

Palomuuri voi tarvittaessa toimia verkon DHCP-palvelimena ja jakaa sisäverkon laitteille niiden tarvitsemat IP-osoitteet automaattisesti, jolloin säästytään siltä, että kaikkien laitteiden IP-osoitteet jouduttaisiin määrittelemään käsin. Isoimmissa verkoissa DHCP-palvelun hoitavat reitittimet tai erillinen DHCP-palvelin, mutta pienemmissä verkoissa palomuuri voi aivan hyvin hoitaa DHCP-palvelimen virkaa.

Palomuuri voi myös julkaista lokitiedostoa yhteyksistä Syslog-serverille, josta näitä tietoja voidaan tarkastella verkonvalvojan toimesta.

7.5 WLAN

Wireless Local Area Network eli tuttavammin langaton lähiverkko on tapa, jolla laitteita voidaan liittää lähiverkkoon langattomasti radiotaajuuksien yli. Yleisesti WLAN-laitteista puhuttaessa tarkoitetaan IEEE 802.11 -sertifioituja laitteita. Muitakin

langattomia standardeja on olemassa, mutta ne eivät ole saavuttaneet suurta suosiota. Suosituimpia 802.11 -standardin versioita ovat 802.11a, 802.11g sekä 802.11n joiden siirtonopeudet ovat 54Mbps, 54Mbps sekä 600Mbps.

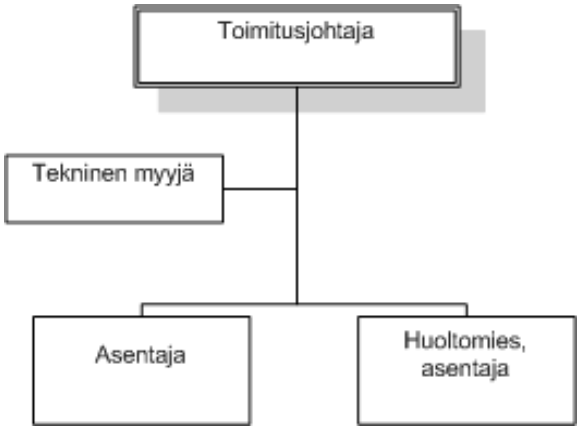
WLAN on kätevä tapa liittää kannettavia tietokoneita sekä WLAN-yhteydellä varustettuja älypuhelimia yrityksen verkkoon, mutta verkon suojauksen kanssa kannattaa olla tarkkana. Vaikkakin WLAN-yhteyksien käyttö niin yritys- kuin kotitalousympäristöissä on lisääntynyt kiinnitetään langattoman verkon tietoturvaan harvemmin sen suurempaa huomiota.

Yrityskäytössä oleva WLAN-verkko tulisi aina suojata käyttäen vähintään WPA- tai WPA2-tasoista salausavainta sekä sen verkkotunnus eli SSID tulisi piilottaa, jotta ulkopuoliset eivät havaitse sitä langattomia verkkoja etsiessään. Tietoturvan maksimoimiseksi voidaan ottaa käyttöön myös verkkosovittimien MAC-osoitteisiin perustuva suodatus, jolloin langattoman yhteyden voivat muodostaa vain ne verkkosovittimet joiden MAC-osoite löytyy reitittimen pääsylistalta. Tätä ominaisuutta kutsutaan nimellä White list.

Samoin WLAN-verkkoa suunnitellessa tulisi ottaa huomioon mahdolliset katvealueet sekä muiden laitteiden verkkoon aiheuttamat häiriöt. Esimerkiksi mikroaaltouuni voi päällä ollessaan häiritä langatonta verkkoa tai tv-kuvan siirtoon langattomasti käytettävät laitteet toimivat yleensä samalla taajuudella, kuin WLAN-laitteet ja näin ollen ne saattavat aiheuttaa ongelmia langattoman verkon toimintaan.

8 TIETOTURVASUUNNITELMA AV-TIIMI LJ OY:LLE

AV-Tiimi LJ Oy on AV-alan erikoisyritys, joka on toiminut jo vuodesta 1993 ja työllistää tällä hetkellä 4 vakituista henkilöä, sekä apulaisia isoihin urakoihin. Yritys keskittyy B2B-kauppaan ja sen asiakkaat ovat suuria julkishallinnon ja yrityselämän toimijoita. Yritys toimittaa AV-laitteita sekä AV-kokonaisuuksia myös ns. "Avaimet Käteen" -periaatteella.



KUVA 8. AV-Tiimin organisaatiokaavio.

Tällä hetkellä yrityksen IT-puolen hoito on teknisen myyjän harteilla. Hän hoitaa varmuuskopioinnin, yrityksen verkkokaupan päivitykset sekä muut IT-asiat. Tiedot varmuuskopioidaan ulkoiselle kiintolevylle, jolle SAP-tietokannan tiedot varmistetaan säännöllisen epäsäännöllisesti.

8.1 Henkilöstöturvallisuus

Kun kyseessä on näinkin pieni yritys, ei sille ole tarpeellista luoda erillistä henkilöstöpolitiikkaa, vaan antaa yrityksessä valloillaan olevan käytännön jatkua. Kaikki työntekijät tuntevat toisensa hyvin ja ongelmia työntekijöiden välille ei ole syntynyt. Samoin työaikana yrityksen tiloissa on yleensä vain 2 henkilöä ja asentajat ovat kentällä asennuksissa. Tämä auttaa osaltaan henkilöstön valvontaa.

Henkilöstö tietää toimenkuvansa ilman, että sitä tarvitsisi erikseen määrittää. Yritys ei myöskään vaadi työntekijöiltään salassapitosopimuksen allekirjoittamista.

Yrityksenä AV-Tiimi ei harjoita mainontaa sosiaalisen median välityksellä. Yrityksen työntekijöilläkään ei ole käyttäjätunnuksia sosiaalisen median palveluihin kuten esimerkiksi Facebookiin tai Twitteriin.

Koska toimintaa sosiaalisen median palveluissa ei ole, on sosiaalisen median kautta leviävien tietoturvauhkien osuus AV-Tiimin tietoturvan kannalta olematon. Tulevaisuudessa mahdollisesti käyttöön otettavissa sosiaalisen median palveluissa tulisi kiinnittää huomiota käyttäjätilin tietoturva-asetuksiin. Vaikkakin kokonaisen sivuston kaappaaminen on vaikeaa, tulisi aina varmistua, että kirjaudutaan oikeaan palveluun. Myöskään yrityksen henkilöstön henkilökohtaisia yhteystietoja ei tulisi sosiaalisessa mediassa levittää. Yrityksen omalla Facebook-tunnuksella voi toki mainosmielessä olla esimerkiksi vaihteen puhelinnumero tai yleinen sähköpostiosoite. Nykyisin Facebook-palvelussa on mahdollista päättää, kuka mitäkin tietoa näkee. Nämä asetukset tulisi viilata siten, että ryhmään kuulumattomille ei näytetä kaikkia tietoja. Epäilyttäviin linkkeihin tai ystäväpyyntöihin tulisi suhtautua varauksella ja mieluummin ne kannattaisi jättää huomioitta.

Jos mahdollista tulisi kaikissa palveluissa käyttää suojattua yhteyttä. Tämä turvaa verkkoliikenteen palveluntarjoajan ja käyttäjän välillä, joka varmistaa sen ettei tärkeitä tietoja pääse ulkopuolisten ulottuville.

8.2 Tiedon tietoturva

Yrityksen sisäinen tiedonvaihto perustuu pitkälti paperilla olevan tiedon siirtämiseen. Tiedonvaihto asiakkaiden ja maahantuojien välillä hoidetaan joko puhelimitse tai sähköisesti sähköpostilla.

Tärkeät esimerkiksi tarjouksiin, myytyihin laitteisiin ja asennuksiin liittyvät sähköpostit tulostetaan. Paperimateriaalin määrän kasvaessa myös dokumenttien hallinta vaikeutuu. Kadonnut asiakirja muodostaa aina aukon yrityksen tietoturvaan. Yrityksessä vierailevа asiakas tai maahantuojan edustaja saattaa nähdä esimerkiksi luottamuksellisia tarjousasiakirjoja tai jälleenmyyjän hinnastoja. Tämä tilanne voidaan ratkaista siten, että työntekijät pitävät työpisteillään vain sillä hetkellä työssään tarvitsemansa dokumentit, toki aina tämä ei ole mahdollista.

Maahantuojien lähettämät sähköiset hinnastot yleensä tulostetaan ja liitetään hinnastoja sisältävään mappiin. Myöskin kaikki myyntilaskut tulostetaan ja lähetetään asiakkaalle joko sähköisenä tai kirjepostina. Tulostettaessa tällaisia yrityksen kannalta arkaluontoisia asiakirjoja on tulostimen sijoituspaikalla suuri merkitys. Yleensä pienempikokoiset tulostimet myös tulostavat paperille siten, että tulostuspuoli jää tulostimessa ylöspäin ja näin osa tulosteesta on kaikkien tulostimen

äärellä liikkuvien luettavissa. Yrityksen verkkotulostin on sijoitettu siten, että matka työpisteiltä laitteelle ei ole pitkä ja se on kuitenkin poissa vieraiden kulkureitiltä.

Niin kutsuttua salasanapolitiikkaa yrityksessä ei ole ja niihin voitaisiinkin kiinnittää yrityksessä huomiota. Osa salasanoista on melko lyhyitä, vaikka ne sisältävätkin kirjaimia sekä numeroita. Erikoismerkkien lisääminen salasanoihin olisi hyvä lisä tietoturvan parantamiseksi, tosin joissain palveluissa erikoismerkkien käyttö salasanoissa voi olla mahdotonta teknisten rajoitusten takia. Saman salasanan käyttö kaikkialla voi luoda tietoturvauhan, jos käytetty salasana saadaan selville.

Huomatessaan, että työasemalla tai palvelimella on virus tai sinne on alkanut ilmestyä outoja tiedostoja ei käyttäjän tulisi hätääntyä. Hätäily ei tällaisissa tilanteissa auta vaan ensin tulisi selvittää minkälaisesta viruksesta tai haittaohjelmasta on kyse ja mitä kaikkea ohjelma tekee. Samoin tulisi selvittää kuinka tästä viruksesta on mahdollista päästä eroon, riittääkö esimerkiksi pelkkä virustutkan tekemä poisto vai joutuuko käyttäjä tekemään jotain muita toimenpiteitä viruksen poistamiseksi. Jos käyttäjä ei omatoimisesti saa virusta poistettua tulisi hänen kirjata mahdollisimman tarkasti milloin hän asian huomasi, kuinka hän asian huomasi, mitä hän on asialle jo tehnyt ja tämän jälkeen ottaa yhteyttä asiantuntevaan henkilöön vian korjaamiseksi.

Käyttäjien olisi hyvä myös tarkkailla käyttämänsä tietokoneen vapaana olevan kiintolevytilan määrää. Jos se alkaa vähentyä huomattavasti ilman käyttäjän toimia, tulisi syy selvittää. Yksi selitys voi toki olla Windows-käyttöjärjestelmä, joka käytön myötä alkaa varata itselleen enemmän tilaa. Toinen voi olla se, että tietokoneelle on pesiytynyt jokin haittaohjelma.

8.3 Varmuuskopiointi

Varmuuskopiointia AV-Tiimissä hoitaa toinen myyjistä. Yritys käyttää SAP Business One -ohjelmistoa. SAP:n käyttämästä tietokannasta otetaan varmuuskopio säännöllisen epäsäännöllisesti, eli lähinnä silloin, kun henkilöllä on muilta töiltään aikaa. Varmuuskopiot otetaan ulkoiselle USB-kiintolevylle, jota säilytetään samassa tilassa palvelimen kanssa.

Varmuuskopiointiratkaisuna tämä ei ole hyvä. Vahingon sattuessa saattaa viimeisin varmuuskopio tietokannasta olla kuukausia vanha. Samoin tulipalon tai muun yrityksen fyysistä tietoturvaa uhkaavan tapahtuman sattuessa ovat myös varmuuskopiot vaarassa tuhoutua.

Ehdotinkin yritykselle varmuuskopiointiratkaisuksi tietoverkkopohjaista NAS-ratkaisua, jolle SAP:n käyttämä tietokanta tallennettaisiin ajastetusti joko päivittäin tai vähintäänkin kerran viikkoon. NAS-järjestelmän etuina voitaisiin pitää sitä, että hankintakustannukset ovat saatavaan hyötyyn nähden maltilliset sekä henkilöstön varmuuskopiointiin käyttämän työmäärän vähentymistä. Kyseinen ratkaisu olisi myös paremmin suojattu vikaantumista vastaan RAID-ominaisuutensa ansiosta. Tällöin toisen laitteessa olevan kiintolevyn menetys ei vielä kadota yrityksen varmuuskopioita vaan siihen vaaditaan molempien levyjen samanaikainen vikaantuminen. Tämän tapahtuman todennäköisyyttä voidaan pitää minimaalisena. Kerran kuussa NAS-järjestelmästä otettaisiin varmuuskopio yrityksen nykyiselle varmuuskopiointiin käyttämälle ulkoiselle USB-kiintolevylle. Tätä ulkoista kiintolevyä tulisi säilyttää poissa yrityksen tiloista esimerkiksi toimitusjohtajan kotona. Tällä taataan se, että jos NAS-järjestelmä tuhoutuu on aina kuitenkin saatavilla jonkinlainen varmuuskopio yrityksen tietokannasta.

Automaattisen tiedonvarmennuksen piiriin laitettaisiin vain SAP:n käyttämä tietokanta. Tarjousasiakirjat, sekä työntekijöiden henkilökohtaiset tiedostot tallennetaan palvelimelle, mutta niiden varmuuskopiointi tapahtuisi käsin. Toki yrityksen näin halutessa myös henkilökohtaiset tiedostot sekä esimerkiksi valmiit tarjoukset voidaan laittaa ajastetun varmuuskopioinnin piiriin.

Nykyisellään yrityksen käyttämä tietokanta vie kiintolevytilaa noin ~600megaa. NAS-laitteeseen suosittelisin hankittavaksi kaksi kappaletta vähintään kahden teratavun kokoista kiintolevyä. Näin varmistetaan se, että levytila ei pääse yllättäen loppumaan.

NAS-järjestelmän voi siis joko hankkia valmiina tai kasata itse. Päädyin suosittelemaan AV-Tiimille valmista NAS-ratkaisua niiden helppokäyttöisyyden vuoksi. Kaupallisen ratkaisun hankkimista puoltaa myös laitteelle annettu takuu sekä asiakastuki mahdollisten ongelmien ilmaantuessa.

Itsekasattu järjestelmä on aina itsekasattu, joskus käy niin hyvin ettei järjestelmä oireile käyttöaikanaan useasti, joskus taas asia on päinvastainen. Itsekasattuun NAS-järjestelmään tarvitaan tarkoitukseen soveltuva tietokone sekä NAS-käyttöön suunniteltu käyttöjärjestelmädistribuutio. Kohdassa 5.1.3 on pintapuolinen esittely eräästä NAS-käyttöön suunnitellusta käyttöjärjestelmästä ja sen ominaisuuksista.

NAS-laitteeksi valitsin QNAP:n valmistaman laadukkaan pienyrityskäyttöön suunnitellun TS-239 Pro II -laitteen. Laitteessa on Intelin valmistama Atom-suoritin sekä 1Gb DDRIII-muistia, sekä kaksi Gigabitin ethernet-liitäntää. Laitteeseen on mahdollista asentaa kaksi maksimissaan kolmen teran kokoista levyä. Näin ollen

siihen on mahdollista saada tallennustilaa joko kuusi teraa tai kolme teraa vikasietoista tallennusta käyttäen. Levyt sijaitsevat omissa kelkoissaan ja ne ovat ns. hot-swap ominaisuudella varustettuja. Hot-swap tarkoittaa sitä, että laite voi olla toiminnassa silloin, kun siihen liitetään uusi kiintolevy. Laitteessa on myös niinkutsuttu online raid –ominaisuus joka tarkoittaa sitä, että kiintolevytilan loppuessa laitteeseen on mahdollista liittää isompi kiintolevy siten, että laite siirtää RAID-pakan ja datan ylläpitoon tarvittavat tiedot ensin toiselle kiintolevylle. Tämän jälkeen kiintolevy voidaan korvata suuremmalla, jonka jälkeen sama toimenpide suoritetaan toiselle kiintolevylle. Samoin käytettyä RAID-tasoa voidaan muutta ilman, että laitteessa olevaa dataa menetetään.

Laitteessa on myös erittäin laajasti muita erilaisia ominaisuuksia:

- Kyky peilata laitteen sisältö toiseen samanlaiseen laitteeseen (Remote Replication)
- Toimia web-serverinä
- Tuki IPv6-verkoille
- Mahdollisuus liittää laitteeseen nauhoittavia IP-valvontakameroita
- Tekstiviesti- sekä sähköpostivaroitukset ongelmatilanteissa
- Rautapohjainen RAID-tuki, RAID-tasot 0, 1.

8.4 Työasemat

Yritys käyttää työntekijöidensä työasemina kannettavia tietokoneita. Käyttöjärjestelminä koneissa on Microsoftin Windows XP, Vista ja Windows 7 -käyttöjärjestelmiä. Kaikkien käyttöjärjestelmien ollessa saman tuoteperheen tuotteita ei yhteensopivuusongelmia esiinny.

Luvatonta käyttöä estämään tietokoneet on suojattu ainoastaan käyttäen Windowsin omaa sisäänkirjautumismenetelmää eli käyttäjätunnusta ja salasanaa. Jokaisen työntekijän käyttäjätunnukset sijaitsevat yrityksen palvelimella ja intranetin käyttöön tarvitaankin nämä Active Directory -palvelussa olevat käyttäjätunnukset. Koneille voidaan toki kirjautua käyttäen koneen järjestelmänvalvojan tunnuksia, mutta palvelimen sisältöön ei tällöinkään päästä käsiksi.

Kaikissa koneissa on tietoturvan parantamiseksi kytketty päälle Windowsin oma Update Service, jotta niiden päivitykset pysyvät aina ajan tasalla. Virustorjunta on

hoidettu kotimaisella F-Securen valmistamalla Internet Security -ohjelmistolla. Myös tässä ohjelmistossa on käytössä automaattinen päivitys -ominaisuus.

8.5 Palvelin

Käyttöjärjestelmänä yrityksen palvelimessa on Microsoftin Small Business Server 2003. Tämä erityisesti pienyritysten palvelinkäyttöön soveltuva käyttöjärjestelmä pitää sisällään monia tarpeellisia palvelinkäytössä tarvittavia ominaisuuksia, kuten esimerkiksi SQL- ja email-palvelut.

Palvelin on sijoitettu omaan lukittavissa olevaan huoneeseensa, johon myös yrityksen kannettavat lukitaan yöksi säilöön. Fyysisen tietoturvan kannalta ratkaisu toki on tyhjää parempi vaikkakaan normaali väliovi ja siinä oleva lukko ei yritykseen tunkeutuvaa varasta pitkään poissa laitetilasta pitäisikään.

Palvelimella on käytössä myös SAP Business One -ohjelmisto, jota yritys käyttää tuoterekisterinsä ylläpitoon, myyntiin sekä laskutukseen. Samoin palvelimelle on asennettu palomuurin luoman syslog-tiedon tarkasteluun sopiva ohjelma, mutta sitä ei ole säädetty kunnolla ja tällä hetkellä ohjelmisto ei kerää ollenkaan tietoa.

Palvelimella toimii SQL-palvelun lisäksi myös Active Directory, joka pitää sisällään käyttäjätiedot käyttäjien sisäänkirjautumista varten. Myös palvelimeen on asennettu F-Securen virustorjuntaohjelmisto, joka suojaa palvelimen virustartunnoilta.

8.6 Tiedon tuhoaminen

Yrityksellä on hankittuna paperiasiakirjojen tuhomista varten asiakirjasilppuri. Asiakirjasilppurin tuottama silppu säkitetään, mikä takaa sen, että se on erittäin vaikeasti koottavissa luettavaksi tekstiksi. CD-/DVD-levyjä yritys käyttää oman tiedon tallentamiseen erittäin harvoin. Optisia levyjä tuhottaessa voidaan ne tarvittessa tuhota fyysisesti rikkomalla levy.

Sähköistä dataa ei yrityksen ole vielä tarvinnut tuhota, mutta helpoin tapa tuhota sähköistä dataa on päällekirjoittaminen. Internetistä on saatavilla ohjelmia, jotka ohittavat käynnistyksessä BIOS:n ja suorittavat ylikirjoituksen käyttäjän haluamalle levy(i)lle. Näin kyseessä olevaa kiintolevyä ei tarvitse tuhota vaan se voidaan

uusiokäyttää. Käytöstä poistuvat kiintolevyt tulisi tuhota mekaanisesti joko purkamalla ne tai käyttämällä voimakasta magneettia levyn demagnetointiin.

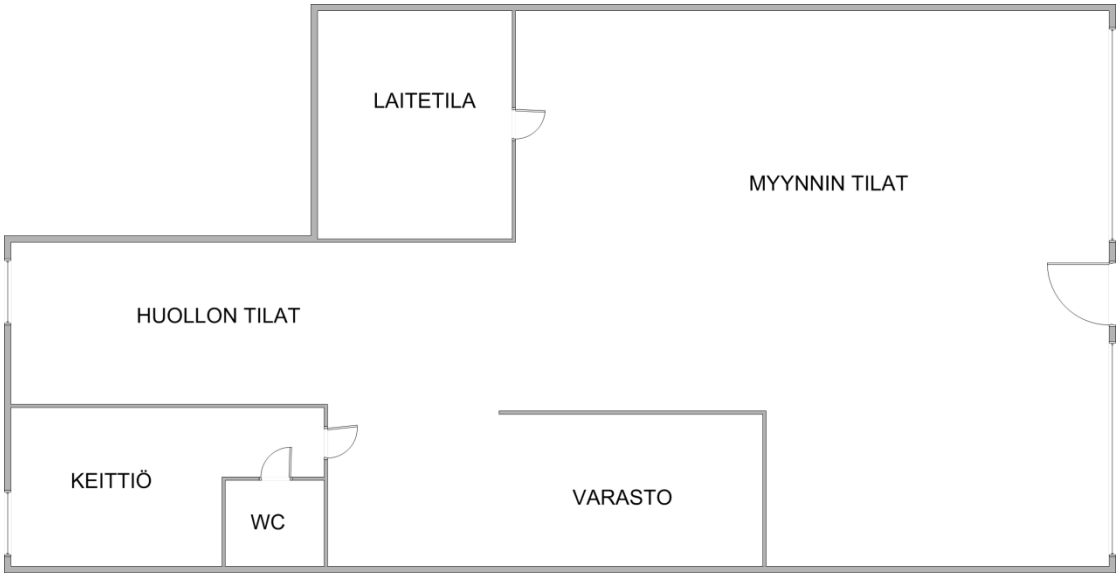
8.7 Yrityksen fyysinen tietoturva

Osa yrityksen tietoturvaa on toimitilojen ja laitteiden fyysinen tietoturva. Tällä pyritään estämään esimerkiksi työntekijöiden tiedon väärinkäyttö, varkaudet ja tulipalot.

Jokaisella työntekijällä on henkilökohtainen avain yritykseen. Henkilöstön omalla vastuulla on se, että avaimesta ei oteta kopioita. Avainten hallinnan merkitystä ei voida korostaa tarpeeksi.

8.7.1 Kulunvalvonta

Yritys käyttää tiloissaan kameravalvontaa. Kamerat kuvaavat sisääntuloreittejä yrityksen tiloihin. Pienet ikkunat on suojattu myös verkolla sisäänpääsyn hankaloittamiseksi. Myynnin työpisteet sijaitsevat sisäänkäynnin molemmin puolin, joten myynnin henkilöstö valvoo työaikanaan myös henkilöiden kulkua yritykseen. Alla olevassa kuvassa on esitettynä yrityksen pohjapiirros. Ratkaisu sopii kyseiselle yritykselle hyvin, sillä se estää asiattomien pääsyn yrityksen liiketiloihin työaikana.



KUVA 9. Pohjapiirros.

8.7.2 Paloturvallisuus

Yrityksen laitetila sijaitsee kuvan 9 osoittamassa paikassa, ja samassa tilassa sijaitsee myös yrityksen lakisääteisesti säilytettäväksi määritelty paperiaineisto. Niitä ovat mm. myynti- ja ostolaskutus *n* vuoden ajalta. Tällainen paperimäärä palvelintilassa lisää tulipalon riskiä, joten näille papereille olisikin hyvä etsiä vaihtoehtoinen säilytyspaikka. Samoin yrityksen paloturvallisuuden parantamiseksi tulisi tiloissa olla ainakin sammutuspeitto sekä jauhe- tai hiilidioksidisammutin. Jos yritykseen hankitaan hiilidioksidisammutin, tulee sitä mahdollisesti käytettäessä ottaa huomioon hiilidioksidin purkautumislämpötila, -76 °C.

Yrityksen tiloissa ei ole paloilmaisia, ja sellaisia olisi hyvä hankkia ainakin palvelintilaan, sillä ovi on yleensä suljettuna ja sieltä mahdollisesti alkava tulipalo huomattaisiin näin aikaisemmin. Huollon puolelle paloilmaisinta ei voida asentaa juotostöiden takia, jotka aiheuttavat savua. Paloilmaisimeksi riittää normaali palovaroitin.

8.7.3 Laitteistoturvallisuus

Yrityksen tietoliikennelaitteet sijaitsevat omalla hyllyllään internet-liitäntään käytettävän puhelinpistokkeen lähettyvillä huollon tiloissa. Laitteita ovat ADSL-modeemi, palomuuri sekä normaali kytkin. Tämä on laitteille sopiva sijoituspaikka, sillä ne eivät ole kenenkään tiellä ja kaapelit saadaan helposti pois kulkureiteiltä. ATK-kaapelointi työpisteille, verkkotulostimelle sekä valvontakameroille kulkee välikatossa, joten sekin on poissa käyttäjien tieltä. Yrityksen ADSL-liittymän toimittaja Sonera on toimittanut yritykseen Cisco-merkkisen ADSL-modeemin. Yrityksen käytössä oleva Draytek Vigor -palomuuri on suojattu salasanalla väärinkäytön estämiseksi. Laitteita ei ole suojattu varkaudelta, mutta laitteiden tekniset ominaisuudet huomioonottaen se ei ole tarpeellista, sillä ne eivät sisällä suojattavaa tietoa. Palvelin sijaitsee omassa huoneessaan, joka on lukittavissa.

8.7.4 Sähkökatko

Palvelinta ei ole suojattu virtapiikeiltä tai sähkökatkoilta ja UPS-laite olisikin suotava hankinta. Se tasoittaisi sähköverkossa tapahtuvia virtapiikkejä ja tarjoaa sähkökatkon sattuessa virtaa palvelimelle siksi aikaa, että se saadaan ajettua hallitusti alas. Laadukkaita UPS-laitteita valmistavat esim. APC sekä Eaton. Suositeltava hankinta

palvelimen virransaannin varmistamiseksi olisi Eaton 5115 UPS -laite, aiemmin markkinoilla laite on ollut nimellä Powerware 5115 UPS.

Työntekijöillä on käytössään kannettavat tietokoneet, jotka sähkökatkon sattuessa toimivat omilla akuillaan sen aikaa, jotta sillä hetkellä auki olleet työt saadaan tallennettua joko palvelimelle tai kannettavan omaan muistiin.

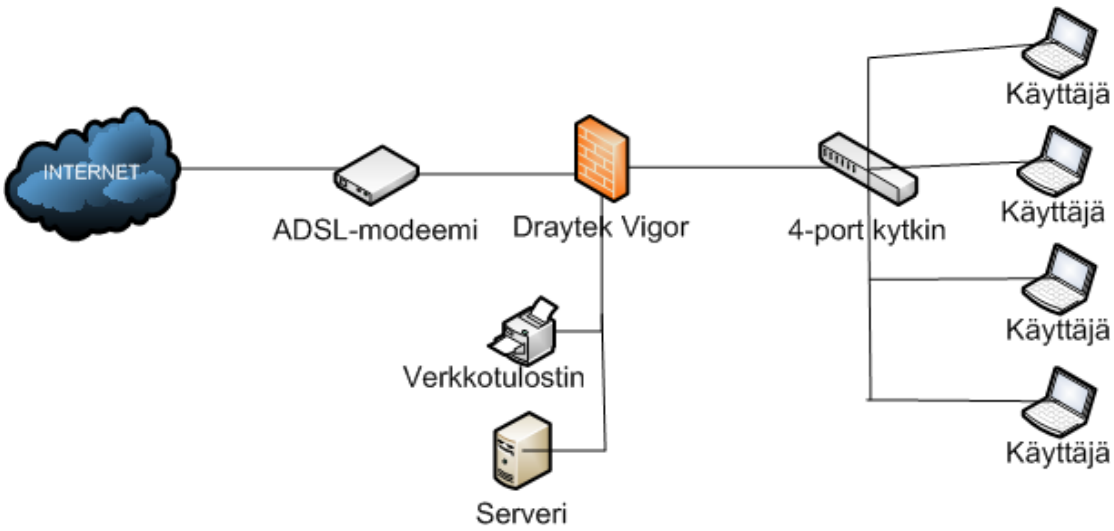
8.8 Tietoverkon tietoturva

AV-Tiimi LJ Oy:ssä tietoverkon tietoturva on ratkaistu hankkimalla Draytek Vigor -merkkinen palomuuri. Palomuuri onkin toiminut hyvin, vaikkakin sillä on jo ikää, mutta sen tarjoamat ominaisuudet ovat rajalliset. Yritys haluaisikin uudistaa tietoverkkoaan siten, että työntekijöillä olisi mahdollisuus käyttää myös VPN-yhteyksiä etätyöskentelyyn.

Sähköpostipalvelut yritys on ulkoistanut Soneralle, joka myös toimittaa yritykselle internet-liitynnän. Näin varmistetaan sähköpostin toimivuus. Myynnin henkilöstö käyttää sähköpostia työaikanaan Microsoftin Outlook-ohjelmistolla, matkakäyttöä varten Soneralla on tarjolla myös selaimella käytettävä www-postipalvelu. Koska Sonera on suuri valtakunnallinen toimija voidaan roskapostisuodatuksen olettaa olevan aina ajantasalla sekä palvelun saatavuutta pitää luotettavana.

Extranet-palvelut, AV-Tiimin tapauksessa verkkokauppa, on myös ulkoistettu. Verkkokauppapalvelun tarjoaa FSP Oy. AV-Tiimin henkilöstön tehtäväksi jääkin vain verkkokaupan päivittäminen, toiminnallisuuteen liittyvät asiat kuuluvat FSP:lle. Tämä vähentää työntekijöiden työmäärää, sillä vikatilanteet ohjautuvat FSP:n ylläpitoryhmälle.

Nykyiset tietoliikennelaitteet tukevat 10 sekä 100megabitin LAN-nopeuksia. Yrityksen tietoverkko on Cat5e-kaapeloitua, jolla on mahdollisuus saavuttaa myös gigabitin yhteysnopeudet LAN-käytössä. Varmuuskopioitavan tietomäärän kannalta nykyinen 10/100-megabitin lähiverkko on riittävän nopea. Tietomäärän kasvaessa hyödytään myös uusien laitteiden 1000megabitin verkkoliitännöistä. Yrityksen verkkotopologia on kuvattu kuvassa 10.



KUVA 10. AV-Tiimin nykyinen verkkotopologia.

VPN-yhteyksien käyttö yrityksessä ei ole onnistunut halutulla tavalla. Tulevaisuutta varten myös palomuuri voitaisiin vaihtaa. Pienyrityskäyttöön sopivia laadukkaita palomuurilaitteita on saatavilla monilta valmistajilta, mm. Cisco sekä ZyXEL. Suositeltava hankinta korvaamaan vanha Draytek Vigor -merkkinen palomuuri olisi ZyXEL ZyWALL USG 100 UTM. Laite tarjoaa monipuoliset palomuuri- sekä VPN-ratkaisut. Kyseisestä laitteesta puuttuu mahdollisuus käyttää WLAN-yhteyttä, mutta yritys ei ole kokenut WLAN:n käyttöä tarpeelliseksi yritystoiminnassaan.

Samalla myös käytössä oleva 4-porttinen kytkin voitaisiin vaihtaa isompaan 10/100/1000-nopeuksiin pystyvään kytkimeen. Tällöin kaikki laitteet saataisiin saman kytkimen portteihin eikä palomuurin portteja tarvitsisi käyttää. Suositeltava hankinta olisi vähintään 8-porttinen, mutta mielellään portteja saisi olla enemmänkin. Näin turvattaisiin tulevaisuudessa mahdollinen verkon kasvu. Kytkin voi olla OSI-mallin toisella tasolla toimiva Layer 2 -kytkin. Laadukkaita kytkinlaitteita valmistavat esimerkiksi Cisco, HP sekä D-Link. Suositeltava hankinta olisi D-Linkin DGS-1210-16 joka tarjoaa 16 kappaletta 10/100/1000Mbps Ethernet-portteja sekä tarpeeksi ominaisuuksia yrityksen tarpeisiin.

8.9 Tietoturvasuunnitelman käyttöönotto

Aloittaessani tietoturvasuunnitelman tekoa oli yrityksen tietoturvassa pienehköjä puutteita. Näistä muutamina voidaan mainita muunmuassa paloilmaisimien puuttumisen ja varmuuskopioinnin hoitamisen. Tarkoitus olisikin ettei tämä tietoturvasuunnitelma jäisi vain ajatustasolle vaan yritys perehtyisi suunnitelmaan ja pyrkisi mahdollisuuksiensa mukaan korjaamaan tietoturvasuunnitelmassa esitetyt

puutteet ja toteuttamaan ehdotettuja ratkaisuja. Tietoturvasuunnitelmassa on otettu huomioon yrityksen mahdollinen kasvu, niin työntekijöiden kuin tietoverkonkin osalta. Siitä löytyy uudelle työntekijälle tarvittavat tiedot sopivasta salasanapolitiikasta sekä esimerkiksi ohjeita oikeanlaiseen varmuuskopiointitapaan.

Toki on muistettava myös se, että mikä tänä päivänä on toimiva ratkaisu ei välttämättä ole sitä enää tulevaisuudessa. Tällöin tietoturvasuunnitelmaa on sovellettava kyseisen ongelman ratkaisemiseksi. Käytetty ratkaisu olisi hyvä kirjata omaan dokumenttiinsa ja lisätä liitteeksi tietoturvasuunnitelmaan. Näin taataan se, että tietoturvasuunnitelma pysyy ajantasalla.

9 AV-TIIMI LJ OY:N LÄHIVERKON SUUNNITTELU

AV-Tiimi LJ Oy tahtoi osana opinnäytetyötäni, että suunnittelisin uudelleen heidän tietoverkkonsa ja siinä käytetyt laitteet.

Tietoverkon suunnittelu ja rakentaminen jaetaan yleensä erilaisiin vaiheisiin. Yleisimmin esiintyvät vaiheet ovat määrittely, suunnittelu, toteutus ja testaus. Määrittelyvaiheessa selvitetään mitä ominaisuuksia tietojärjestelmältä vaaditaan. Tämän voi toteuttaa esimerkiksi kartoituksin ja analyysein. Määrittelyvaihetta määrittää olennaisesti se, että ollaanko suunnittelemassa täysin uutta vai korvaamassa vanhaa järjestelmää tehokkaammalla ratkaisulla.

Suunnitteluvaiheessa pyritään löytämään ratkaisut määrittelyvaiheessa asetetuille tavoitteille. Suunnitteluvaiheessa on hyvä vertailla erilaisia vaihtoehtoja, kustannuksia, hyötyjä ja niin edelleen. Suunnitteluvaiheessa huomataan yleensä myös, että jotkin määrittelyvaiheessa halutut ominaisuudet ovat mahdottomia toteuttaa. Suunnitteluvaiheessa olisi hyvä myös noudattaa, mahdollisuuksien mukaan, kansainvälisiä standardeja sillä ne helpottavat tulevaisuudessa tehtäviä muutoksia.

Toteutusvaiheessa tietojärjestelmä toteutetaan varsinaisesti. Yleensä toteutusvaiheessa tulee eteen myös tilanteita, joissa huomataan suunnitteluvaiheen asioiden olevan ristiriidassa toteutuksen kanssa ja tällöin suunnitelmaa joudutaan joidenkin kohtien osalta muuttamaan.

Testausvaiheiissa varmistetaan, että tietojärjestelmä ja verkko toimivat halutulla tavalla.

Kaikista vaiheista tulisi suorittaa mahdollisimman kattava dokumentointi järjestelmän tulevia käyttäjiä sekä ylläpitäjiä varten. Tämä helpottaa verkon kasvattamista ja muutosten tekemistä tulevaisuudessa, kun ylläpitäjän ei tarvitse käyttää turhaa aikaa asioiden selvittämiseen.

Määrittelyvaiheessa tuotetaan yleensä määrittelydokumentti, joka kertoo yksityiskohtaisesti järjestelmältä vaaditut ominaisuudet. Suunnitteluvaiheen dokumentteihin kirjataan ne ratkaisut joilla haluttuihin ominaisuuksiin päästään. Toteutusvaiheen dokumentointi onkin yksi tärkeimmistä dokumenteista joita tietoverkon rakentamisessa tuotetaan sillä se kertoo tehdyt asetukset ja tarvittaessa kommentoi niitä. Toteusvaiheen dokumenteissa oletetaan, että niiden lukija tietää mistä asiasta on kyse, joten niiden ei tarvitse olla asennusohjeen tyyppisiä "tee-näin-

ja-näin"-lehtisiä. Testausvaiheen dokumentteihin kirjataan käytetyt testausmenetelmät sekä vähintäänkin testin lopputulos.

Opinnäytetyössäni AV-Tiimin tietoverkko määritellään ja suunnitellaan, toteutuksen sekä testauksen jäädessä tulevaisuuteen. Määrittelyssä ja suunnittelussa pyrin ottamaan huomioon mahdollisimman paljon jo yrityksessä nykyisin käytettyjä tapoja sekä tuoda mukaan uutta näkemystä siitä, kuinka asia voitaisiin toteuttaa.

9.1 Määrittely

Tietoverkon kaapelointina AV-Tiimissä käytetään tällä hetkellä cat5e-standardoitua ethernet-kaapelia, jolla on mahdollista saavuttaa 1Gbps:n siirtonopeudet. Tällä hetkellä verkossa siirretty tietomäärä ei muodosta ongelmaa edes hitaissa 10Mbps:n verkoissa, mutta tulevaisuutta ajatellen on aina hyvä, että on olemassa jonkinlaista reserviä siirtokapasiteetin suhteen. Yrityksen toimitiloissa ei alunperin ole ollut yleiskaapelointia, eli vuokralaisen on suunniteltava ethernet-kaapelointi itse. AV-Tiimin vaihtuessa kyseisen tilan vuokralaiseksi ratkaistiin kaapelointiongelma silloin siten, että käytetyt kaapelit nostettiin laitehyllyn kohdalta välikattoon, jossa ne kuljetettiin työpisteille sekä tulostimelle ja laskettiin alas. Tämä on osoittautunut varsin toimivaksi ratkaisuksi ja ulkopuolisilta häiriöiltä, jotka voisivat vaikuttaa kaapeliin on säästytty. Uusia kaapelivetoja joudutaan NAS-laitteen takia tekemään. Olen suunnitellut, että NAS-laitteen molemmat verkkoliitännät otetaan käyttöön jolloin saadaan redundanttinen verkkoliityntä NAS-laitteelle joka takaa varmuuskopioinnin onnistumisen kaapelirikon tai verkkokortin rikkoontuessa. Yleisesti myös verkon kriittiset laitteet tulisi varmistaa redundanttisesti, mutta ottaen huomioon yritykselle koituvat kulut sekä ratkaisun käytännöllisyyden ei laitteiden kahdentamisella saavuteta sellaista hyötyä, että se olisi kannattavaa. Yrityksellehän toki jäävät vanhat tietoliikennelaitteet voidaan ottaa uusiokäyttöön, jos jokin uusista laitteista vikaantuu.

Nykyisin käytetyt laitteet tukevat 10/100Mbps:n verkkoliityntää, mutta tietoturvasuunnitelmassani olen jo esitellyt uudet, korvaavat laitteet. Verkossa tapahtuva dataliikenne on tällä hetkellä vain hetkittäistä, pienissä purskeissa tapahtuvaa tiedonsiirtoa. Verkossa siirretään pieniä tekstidokumentteja, kuvia ja sen sellaisia, jotka eivät vaadi verkolta paljon suorituskykyä. Tietoturvasuunnitelmassani esitetty NAS-ratkaisu taas tulisi siirtämään isoja tiedostoja yhtäjaksoisesti verkon yli palvelimelta NAS-laitteella, joka vaatii verkolta lähinnä vakaata toimintaa eikä niinkään nopeutta. Tämä sen takia, että varmuuskopiointi voidaan määrittää tapahtuvaksi öisin jolloin muuta liikennettä lähiverkossa ei ole ja aikaakin tiedostojen

siirtoon on tunteja jolloin vähän hitaampikin verkko kyllä riittää. Mitä nopeammin tiedosto saadaan talteen siirtymään sitä turvallisempi ratkaisu toki on.

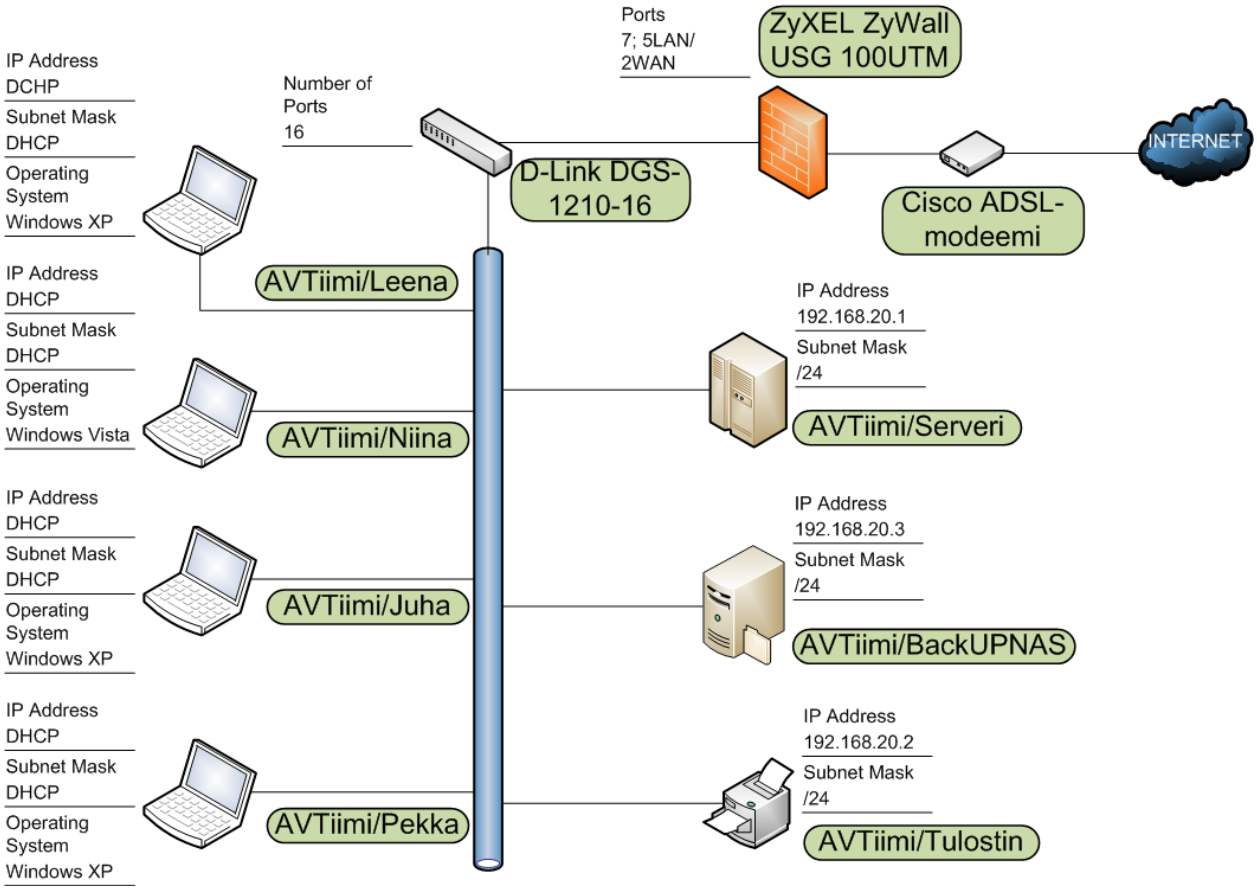
Verkossa ainakin tarvittavat palvelut ovat: osoitepalvelu (DHCP), etäkäyttö (VPN) sekä NAT.

Laitteita jotka käyttävät verkkoa ovat: palvelin, verkkotulostin, NAS-laite sekä neljä työasemaa. Langattoman lähiverkon hyödyntämistä yritys ei katso tarpeelliseksi, mutta sekin ominaisuus on tähän suunnitelmaan helposti lisättävissä. WLAN:lle käyttöä tuskin olisi, ellei maahantuojien satunnaisesti tapahtuvia vierailuja tai tulevaisuudessa työntekijöille mahdollisesti hankittavia älypuhelimia oteta huomioon.

Ulkoverkkoon liitytään Soneran toimittaman ADSL-liittymän avulla. Yrityksen tiloissa sijaitsee Soneran toimittama siltaavassa tilassa oleva ADSL-modeemi.

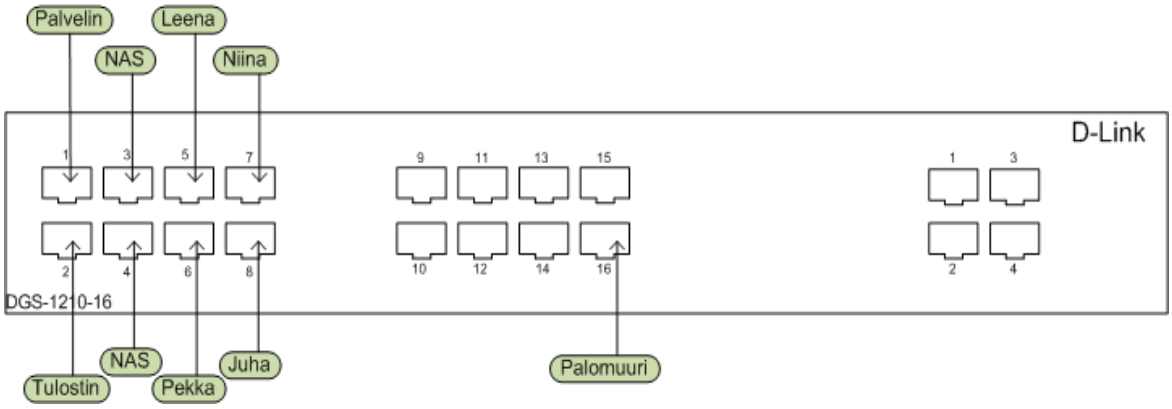
9.2 Suunnittelu

Verkon suunnittelussa painotin uudistuneen topologian järkevyyttä sekä laitteiden mahdollisimman tehokasta käyttöä. Tietoturvasuunnitelmassa esitetyt kytkin- sekä palomuurilaite ovat mitoitettu hiukan yläkanttiin yrityksen kokoa ajatellen. Näin myös tulevaisuutta ajatellen on olemassa laajennusvaraa ilman laitteiden turhaa uusimista. Alla olevassa kuvassa (kuva 11) olen esittänyt verkon uudistuneen topologian missä kuvataan laitteet ja niistä hiukan informaatiota.



KUVA 11. Uudistuneen verkon topologia.

Palomuuriin ei siis kytketä muuta kuin kytkin sekä ulkoverkkoliityntä. Kytkimeen kytketään kaikki ICT-laitteet. NAS-laite tarvitsee kaksi porttia reduntanttisen yhteyden varmistamiseksi. Serverikone, NAS sekä verkkotulostin tarvitsevat omat, kiinteät, IP-osoitteet. Työasemille IP-osoitteet voidaan jakaa DHCP-palvelun välityksellä automaattisesti. Alla olevassa kuvassa olen kuvannut kytkimen portit sekä se mihin porttiin mikäkin laite liitetään.



KUVA 12. Kytkinliitännät.

Kuten kuvasta käy ilmi, jää kytkimeen 7 porttia tyhjää tilaa tulevaisuuden laitteita varten.

IP-osoitteisto hoidetaan käyttämällä C-luokan yksityistä verkkoa ICT-laitteiden osoitteistona. Toki B- tai A-luokan yksityistä verkkoa voitaisiin käyttää, mutta yrityksen koon huomioonottaen jo C-luokan yksityinen verkko on valtavan suuri. Valittu verkko on 192.168.20.xxx. Ensimmäiset kymmenen osoitetta varataan kiinteiksi IP-osoitteiksi niitä tarvitsevia laitteita varten. Loput osoitteet voidaan jakaa DHCP:llä laitteille. Tämä on kuvattu selkeämmin taulukossa 1.

TAULUKKO 1. Laitteiston IP-osoitteet.

LAITE	IP-Osoite	Aliverkon peite
Palvelin	192.168.20.1	255.255.255.0
Tulostin	192.168.20.2	255.255.255.0
NAS	192.168.20.3	255.255.255.0
(Kiinteät)	192.168.20.4 - .10	255.255.255.0
DHCP	192.168.20.11 - .254	255.255.255.0

Ulkoverkon osalta käytetään NAT-palvelua, jolloin yksi julkinen IP-osoite riittää.

Palomuurissa on kaksi erilaista mahdollisuutta toteuttaa VPN-yhteydet. Joko WWW-pohjainen SSL VPN tai perinteisempi menetelmä joka käyttää IPSeciä. SSL VPN on näistä kahdesta turvallisempi ratkaisu, mutta laitteen mukana toimitetaan vain 2 lisenssiä ohjelmistoon jolla VPN:ää käytetään. En pitäisi tätä kuitenkaan suurena haittana sillä tällä hetkellä ainoat henkilöt jotka etäkäyttönä SAP:a haluaisivat käyttää ovat myynnin henkilöt, joita tällä hetkellä yrityksessä työskentelee 2 kappaletta. Käyttäjän koneelle ei siis tarvitse SSL VPN:n tapauksessa asentaa mitään ohjelmistoja etäyhteyden käyttöön vaan se tarvitsee vain WWW-selaimen jossa on Java-tuki, joka nykypäivänä löytyy jokaiselta koneelta. IPSec-VPN:ä varten tarvitsee käyttäjän hankkia koneelleen erillinen ohjelmisto, jonka avulla VPN-yhteys muodostetaan. ZyXEL tarjoaa tähän omaa VPN-yhteysohjelmaansa.

Kustannusten osalta olen pyrkinyt valitsemaan laitteita, joita yritys voi hankkia jo sen olemassaolevilta yhteistyökumppaneilta, ainut poikkeus tähän on ehdottamani NAS-laite. Laitteiden hankintakustannukset on esitetty taulukossa 2, hinnat ovat kuluttajahinnoista muodostettuja arvioita ja ne voivat muuttua. NAS-laitteen hinnassa ei ole laskettu mukaan siihen hankittavia kiintolevyjä, jotka muodostavat noin 150 – 250€ lisäkulun kiintolevyjen koosta riippuen.

TAULUKKO 2. Laitteiden hankintakustannukset.

LAITE	Hankintahinta (alv0%)
ZyXEL ZyWALL 100 USG	420,00 €
D-Link DSG-1210-16	195,00 €
Q-NAP TS-239PRO II	430,00 €
Kokonaiskustannus:	**1 045,00 €**

Kysymys on siis jo melko mittavasta hankinnasta, kun otetaan huomioon yrityksen koko. Uudistetun verkon elinkaaren voidaan kuitenkin olettaa olevan vähintään 5-6vuotta ellei enemmänkin jolloin hankintakustannus suhteutettuna käyttöikään jää todella kohtuulliseksi.

10 YHTEENVETO

Opinnäytetyössä suunniteltiin AV-alaan erikoistuneelle keravalaiselle yritykselle tietoturvasuunnitelma, verkkopohjainen tiedonvarmennusratkaisu sekä nykyisen tietoverkon uudistaminen.

Yritykselle on tässä työssä luotu uusi käytäntö sekä toimintamalli tietoturvaan liittyvien kysymysten ratkaisemiseen. Suunnitelmassa otettiin kantaa esimerkiksi toimivaan salasanapolitiikkaan sekä opastettiin käyttäjiä hyvään varmuuskopiointitapaan.

Työstä syntyneitä dokumentteja ovat tietoturvasuunnitelman lisäksi NAS-järjestelmän sekä tietoverkon uudistuksen suunnittelu- sekä määrittelydokumentit.

Työn tavoite saavutettiin. Yrityksen tietoturvaa kehitettiin luomalla uusi käytäntö toimia, mutta tietoturva parantuu vain jos esitettyjä ratkaisuja toteutetaan ja noudatetaan. Suositeltiin myös ehdotuksia varmuuskopioinnin levytilan kasvattamiseen sekä varmuuteen liittyvissä kysymyksissä. Tietoverkon uudistus sekä varmuuskopiointiratkaisun toteuttaminen jäivät yrityksen tulevaisuuden tehtäviksi.

LÄHTEET

Fried, S. 2010. *Mobile Device Security – A comprehensive guide to securing your information in a moving world*, Boca Raton, FL: Auerbach Publications.

Hakala, M., Vainio, M. 2005. *Tietoverkon rakentaminen*. Jyväskylä: Docendo.

Litmanen, L. 2010. *Information security plan for a small company.* Kuopio: Savonia University of Applied Science, Information Technology, Bachelor of Engineering. Thesis.

Panda Security, *1st AnnualSocial Media Risk Index forSmall to Medium Sized Businesses* [verkkodokumentti], 2010 [viitattu 20.1.2011] saatavilla http://press.pandasecurity.com/usa/wp-content/uploads/2010/09/1st-Annual-Social-Media-Risk-Index.pdf

Raggad, Bel G. 2010. *Information Security Management.* Boca Raton, FL: Auerbach Publications.

Ruohonen, M. 2002. *Tietoturva.* Jyväskylä: Docendo.

Tenhunen, H. 2008 *Modeling the Commissioning of the SAN (Storage Area Network) Disk System*. Kajaani: Kajaani University of Applied Sciences, Master's Degree for Technology Competence Management. Thesis.

Valtiovarainministeriö, *Tärkein tekijä on ihminen – Henkilöstöturvallisuus osana tietoturvallisuutta* [verkkodokumentti]. Edita. Helsinki. 2008. [viitattu 9.1.2011] saatavilla http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20080218Taereki/Vahti2_08low.pdf

Valtiovarainministeriö, *Tietoteknisten laitetilojen turvallisuussuotitus* [verkkodokumentti], Helsinki. 2002. [viitattu 15.1.2011] saatavilla http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20020101Tietot/turvallisuussuositus.pdf

Valtiovarainministeriö, *Sosiaalisen median tietoturvaohje* [verkkodokumentti], Helsinki. 2010. [viitattu 20.1.2011] saatavilla http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101222Sosiaa/Sosiaalinen_media.pdf

www.savonia.fi

Savonia
ammattikorkeakoulu